CLI Manual

Product Model :

DGS-3200 Series

Layer 2 Gigabit Ethernet Managed Switch

Release 1.35

.

March 2009

651GS320025G

RECYCLABLE

Table of Contents

I. Introduction

The Introduction section includes the following chapter: Using Command Line Interface.

1 Using Command Line Interface

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

This manual provides a reference for all of the commands contained in the CLI. 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 User Manual. For detailed information on installing hardware please also refer to the User Manual.

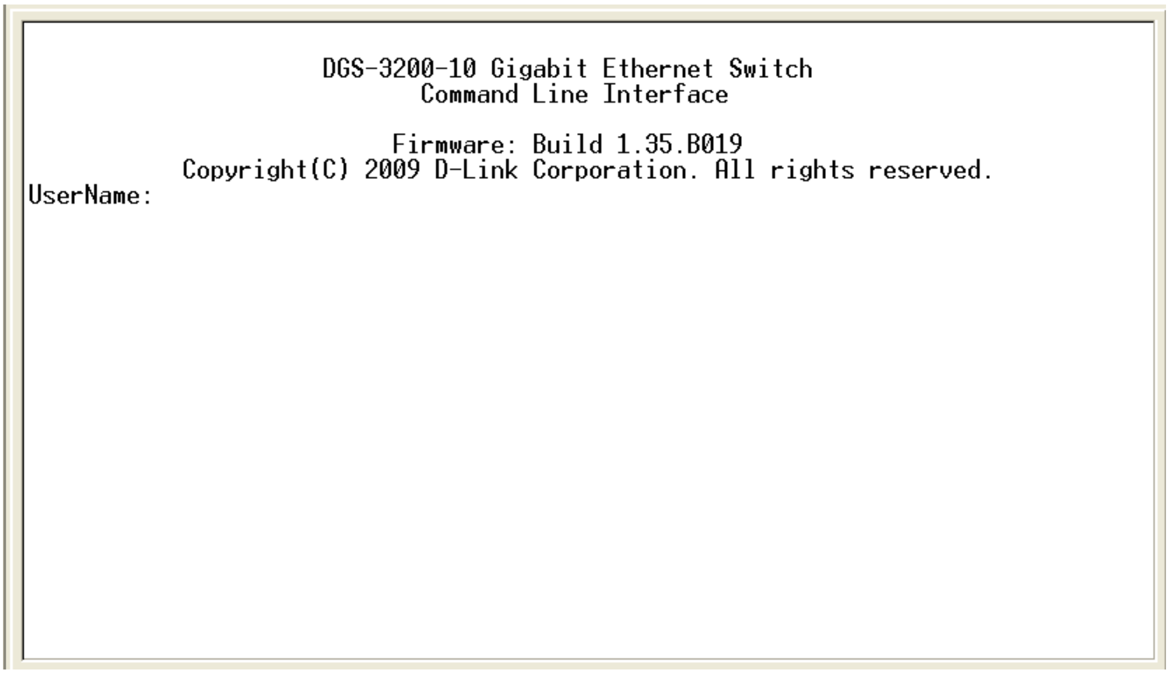
1-1 Accessing the Switch via the Serial Port

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 RS-232 DB-9 cable.

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



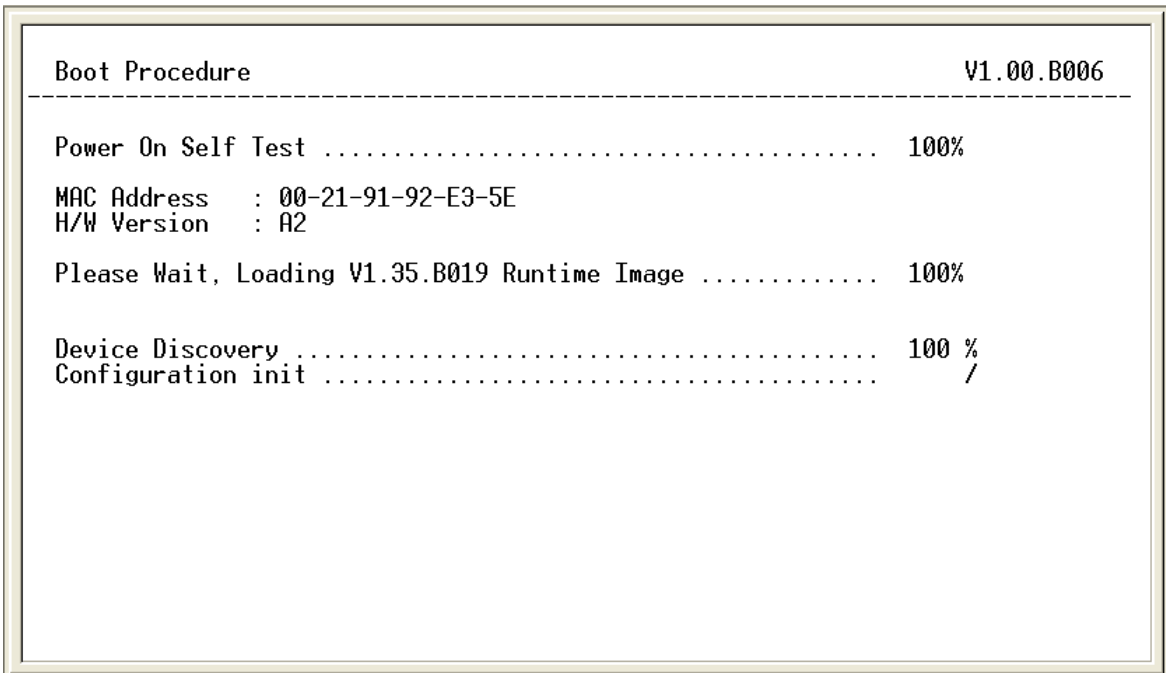
```
                          DGS-3200-10 Gigabit Ethernet Switch
                               Command Line Interface

                               Firmware: Build 1.35.B019
              Copyright(C) 2009 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-3200-10:4#**. 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.B006
------------------------------------------------------------------------------

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

MAC Address   : 00-21-91-92-E3-5E
H/W Version   : A2

Please Wait, Loading V1.35.B019 Runtime Image ............  100%


Device Discovery .........................................  100 %
Configuration init .......................................      /
```

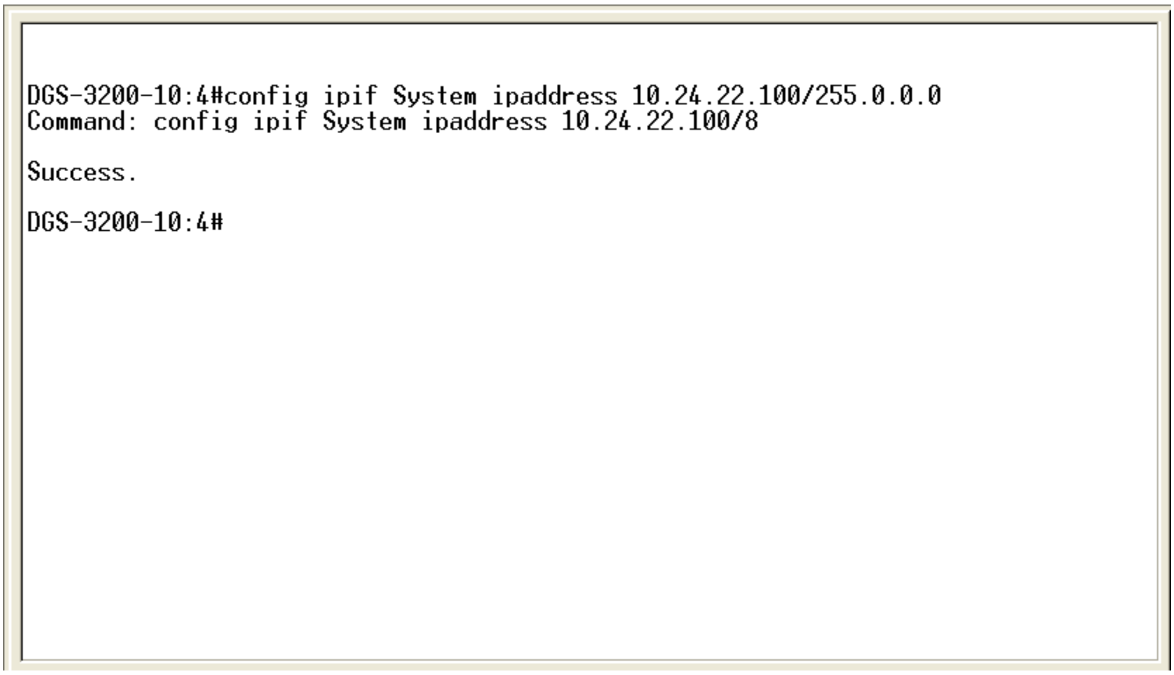
The Switch's MAC address can also be found in the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.

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

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

1. 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.
2. 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.

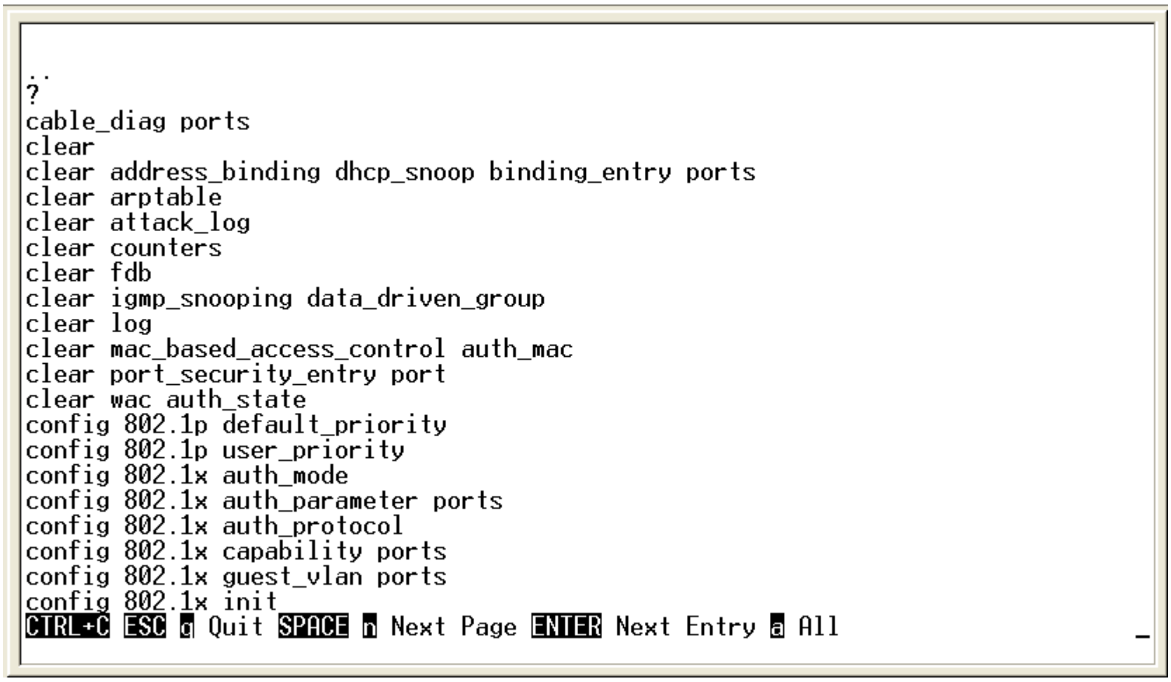
The IP interface named **System** on the Switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the Switch's Telnet or Web-based management agent



```
DGS-3200-10:4#config ipif System ipaddress 10.24.22.100/255.0.0.0
Command: config ipif System ipaddress 10.24.22.100/8

Success.

DGS-3200-10:4#
```

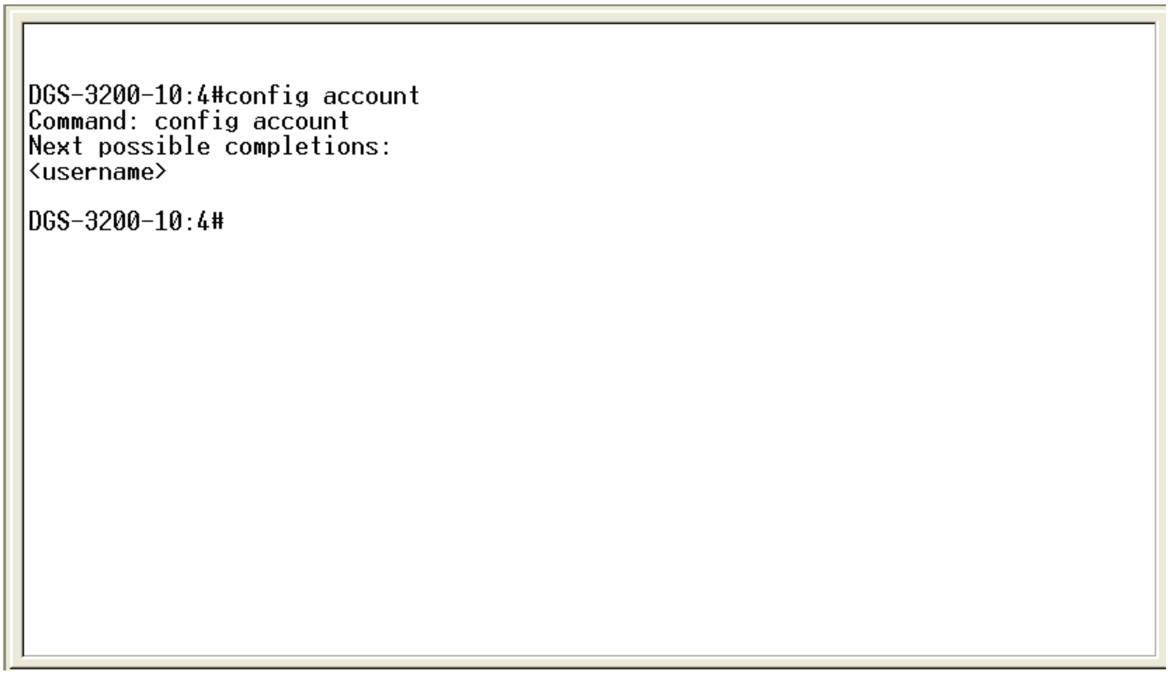
In the above example, the Switch was assigned an IP address of 10.24.22.100 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet, SNMP MIB browser and the CLI or via the Web-based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

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



```
..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear fdb
clear igmp_snooping data_driven_group
clear log
clear mac_based_access_control auth_mac
clear port_security_entry port
clear wac auth_state
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
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.

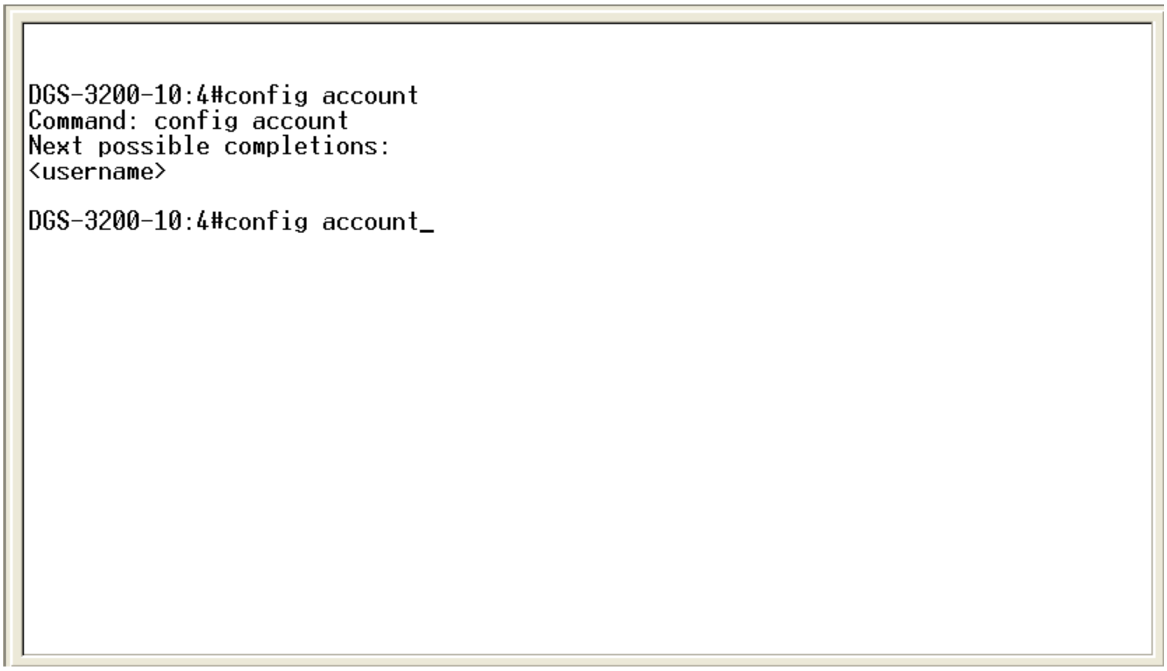


```
DGS-3200-10:4#config account
Command: config account
Next possible completions:
<username>

DGS-3200-10:4#
```

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.

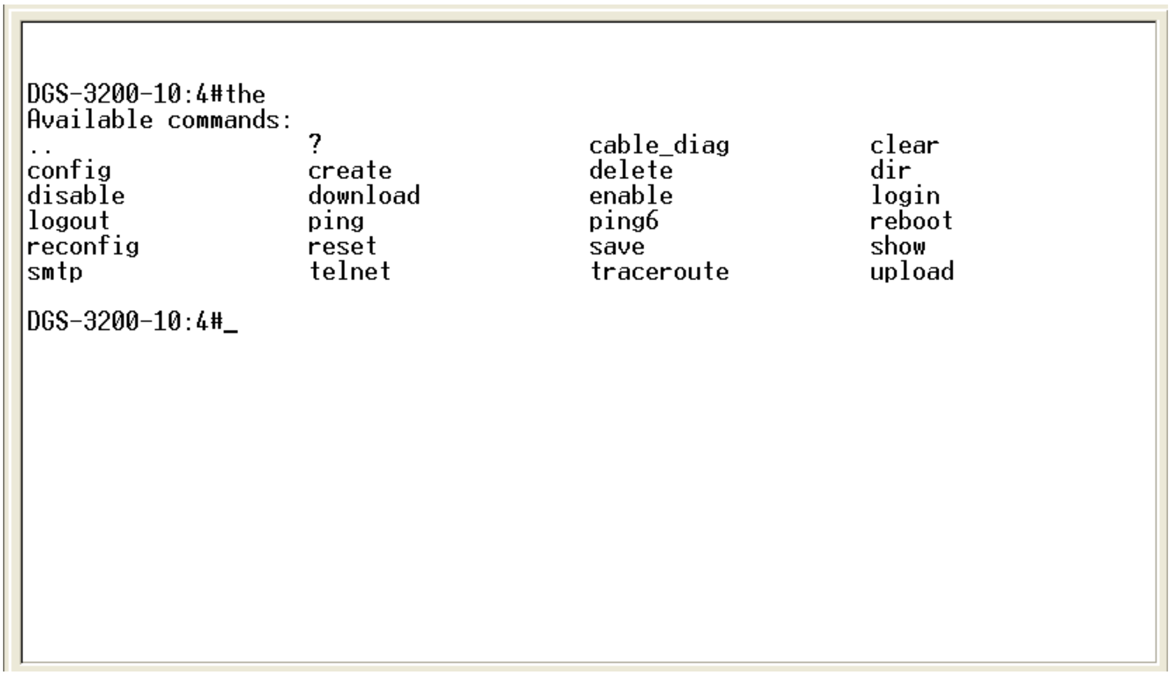


```
DGS-3200-10:4#config account
Command: config account
Next possible completions:
<username>

DGS-3200-10:4#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.

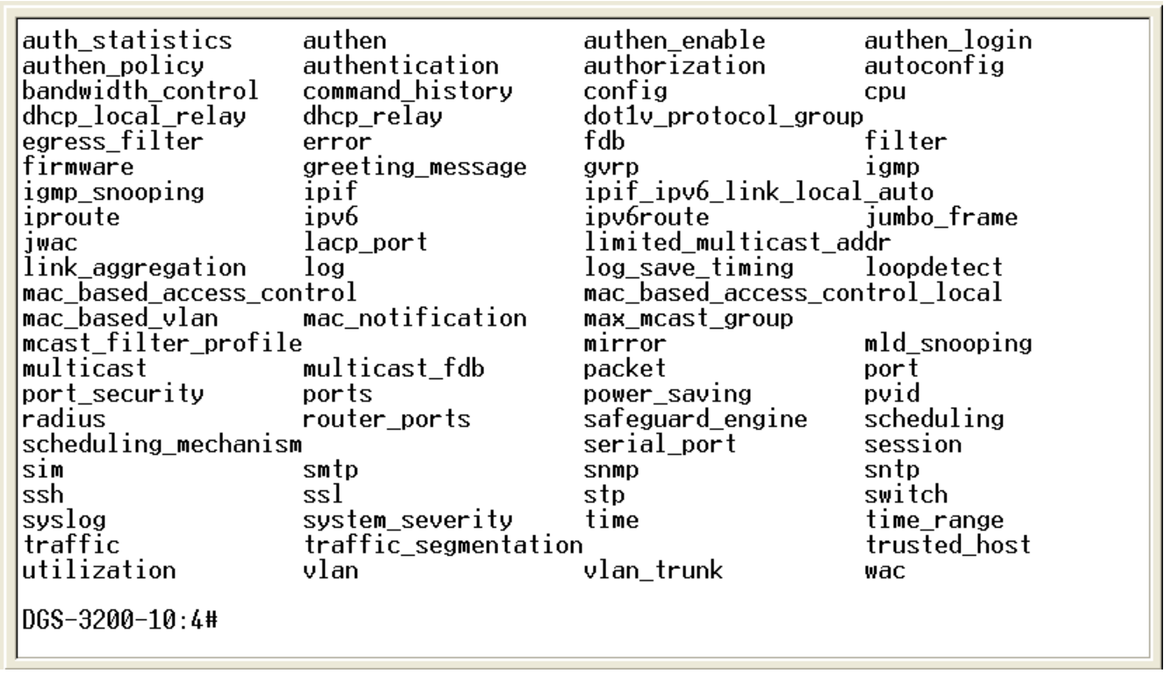
If a command is entered that is unrecognized by the CLI, the top-level commands will be displayed under the **Available commands:** prompt



```
DGS-3200-10:4#the
Available commands:
..                  ?                   cable_diag          clear
config              create              delete              dir
disable             download            enable              login
logout              ping                ping6               reboot
reconfig            reset               save                show
smtp                telnet              traceroute          upload

DGS-3200-10:4#_
```

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.



```
auth_statistics     authen              authen_enable       authen_login
authen_policy       authentication      authorization       autoconfig
bandwidth_control   command_history     config              cpu
dhcp_local_relay    dhcp_relay          dot1v_protocol_group
egress_filter       error               fdb                 filter
firmware            greeting_message    gvrp                igmp
igmp_snooping       ipif                ipif_ipv6_link_local_auto
iproute             ipv6                ipv6route           jumbo_frame
jwac                lacp_port           limited_multicast_addr
link_aggregation    log                 log_save_timing     loopdetect
mac_based_access_control                mac_based_access_control_local
mac_based_vlan      mac_notification    max_mcast_group
mcast_filter_profile                    mirror              mld_snooping
multicast           multicast_fdb       packet              port
port_security       ports               power_saving        pvid
radius              router_ports        safeguard_engine    scheduling
scheduling_mechanism                    serial_port         session
sim                 smtp                snmp                sntp
ssh                 ssl                 stp                 switch
syslog              system_severity     time                time_range
traffic             traffic_segmentation                    trusted_host
utilization         vlan                vlan_trunk          wac

DGS-3200-10:4#
```

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

angle brackets <>	Enclose a variable or value. You must specify the variable or value. For example, in the syntax **create ipif <ipif_name 12> <network_address> <vlan_name 32> {secondary | state [enable | disable]}** you must supply an IP interface name for **<ipif_name 12>** ,a vlan name for **<vlan_name 32>** and an address for **<network_address>** when entering the command. Do not type the angle brackets.
square brackets [ ]	Enclose a required value or list of required arguments. One or more values or arguments must be specified. For example, in the syntax **create account [admin | user]** you must specify either the admin-level or user-level account when entering the command. Do not type the square brackets.
vertical bar |	Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax **show snmp [community | traps]** you must specify either the community or trap receiver in the command. Do not type the vertical bar.

braces { }	Enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax **reset { [config | system] }** you may choose config or system in the command. Do not type the braces.
Ipif <ipif_name 12> **metric <value 1-31>**	12 means the maxmum length of IP interface name. 1-31 means the legal range of metric value.

1-4 Line-Editing Keys

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

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

II. Interface and Hardware

The Interface and Hardware section includes the following chapter: Switch Port and Cable Diagnostics.

2 Switch Port Command List

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

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

2-1 config ports

Purpose

To configure the switch port settings.

Format

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

Description

This command is used to change switch port settings.

Parameters

Parameters	Description	
portlist	Specified a range of ports to be configured.	
all	To set all ports in the system, you may use **all** parameters.	
medium_type	Specify the medium type when configuring ports that are combo ports. This is an optional parameter for configuring the medium type of a combo port; If there are no combo ports, user need not specify **medium_type** in the command.	
Speed	You can set port speed for the specified ports .	
	auto	Set port speed to auto negotiation.
	10_half	Set port speed to 10_half.
	10_full	Set port speed to 10_full.
	100_half	Set port speed to 100_half.
	100_full	Set port speed to 100_full._

	1000_full	**1000_full** sets port speed to 1000_full. When setting port speed to **1000_full**, user should specify master or slave mode for 1000 base TX interface, and leave the **1000_full** without any master or slave setting for other interface.
flow_control	You can turn on or turn off flow control on one or more ports by setting **flow_control** to enable or disable.	
learning	You can turn on or turn off MAC address learning on one or more ports.	
state	Enables or disables the specified port. If the specified ports are in error-disabled status, configuring their **state** to **enable** will recover these ports from a disabled to an enabled state.	
description	Describes the port interface.	
clear_description	Deletes the present description of the port interface	

Note: Gigabit Ethernet ports are statically set to 1 Gbps and their speed cannot be modified.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the speed of ports 1 to 3 of unit 1 to be 10 Mbps, with full duplex, learning enabled, state enabled, and flow control enabled:

```
 DGS-3200-10:4# 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-3200-10:4#
```

2-2 show ports

Purpose

To display the current configurations of a range of ports.

Format

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

Description

This command is used to display the current configurations of a range of ports. If no parameter is specified, all ports will be displayed.

Parameters

Parameters	Description
portlist	Specified a range of ports to be displayed.
description	Indicate if port description will be included in the display .
err-disabled	Indicate if ports are disabled by some reasons will be displayed.
	Note: If no parameter is specified, all ports will be displayed.

Restrictions

None.

Example

To display the configuration of ports 1 to 4:

```
DGS-3200-10:4#show ports 1-4
Command: show ports 1-4

Port     Port          Settings             Connection          Address
         State    Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
------  --------  ---------------------  ---------------------  ---------
1       Enabled   Auto/Disabled           100M/Full/None        Enabled
2       Enabled   Auto/Disabled           Link Down             Enabled
3       Enabled   Auto/Disabled           Link Down             Enabled
4       Enabled   Auto/Disabled           Link Down             Enabled

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-3200-10:4#show ports 1-4 description
Command: show ports 1-4 description

Port     Port           Settings             Connection          Address
         State    Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
------  --------  ---------------------  ----------------------  --------
1       Enabled   Auto/Disabled          100/Full/None            Enabled
         Description:
2       Enabled   Auto/Disabled          Link Down                Enabled
         Description:
3       Enabled   Auto/Disabled          Link Down                Enabled
         Description:
4       Enabled   Auto/Disabled          Link Down                Enabled
         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-3200-10:4#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-3200-10:4#
```

3 Cable Diagnostics Command List

cable_diag ports [<portlist>| all]

3-1 cable_diag ports

Purpose

To test copper cables. If there is an error on the cable, the type of error can be determined and the position where the error occurred.

Format

cable_diag ports <portlist>

Description

This command is used to test copper cabling. For 10/100Based-TX link speed RJ45 cable, two pairs of cable will be diagnosed. For 1000Base-T link speed RJ45 cable, four pairs of cable 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, and crosstalk means that the cable in the error pair has a crosstalk problem at the specified position.

When a port is in link-up status, the test will obtain the distance of the cable. Since the status is link-up, the cable will not have the short or open problem. The test may still detect the crosstalk problem, however. When a port is in link-down status, the link-down may be caused by many factors.

When the port has a normal cable connection, but the remote partner is powered off, the cable diagnosis can still diagnose the health of the cable as if the remote partner is powered on. When the port does not have any cable connection, the result of the test will indicate no cable. The test will detect the type of error and the position where the error occurs.

Note that 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.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be tested.

Restrictions

Only Administrator-level users can issue this command.

Example

To test the cable on ports 1 to 4, and 8:

```
DGS-3200-10:4# cable_diag ports 1-4, 8
Command: cable_diag ports 1-4, 8
Perform Cable Diagnostics ...

 Port     Type         Link Status          Test Result      Cable Length(M)
 ---- ------------ ----------------  ---------------------- -------------
  1     1000Base_T     Link Up       OK                             4
  2     1000Base_T     Link Down     No Cable                       -
  3     1000Base_T     Link Down     No Cable                       -
  4     1000Base_T     Link Down     No Cable                       -
  8     1000Base_T     Link Down     No Cable                       -


DGS-3200-10:4#
```

III. Fundamentals

The Fundamentals section includes the following chapters: Basic Management, Utility, and Power Saving.

4 Basic Management Command List

```
create account [admin | user] <username 15>
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
show serial_port
config serial_port { baud_rate [ 9600 | 19200 | 38400 | 115200 ] |
auto_logout[ never|2_minutes|5_minutes|10_minutes|15_minutes] }
enable clipaging
disable clipaging
enable telnet {<tcp_port_number 1-65535>}
disable telnet
enable web {<tcp_port_number 1-65535>}
disable web
save {[config <config_id 1-2> | log | all]}
reboot
reset {[config | system ]}
login
logout
```

4-1 create account

Purpose

To create user accounts

Format

create account [admin | user] <username 15>

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 account (include admin and user) is up to 8.

Parameters

Parameters	Description
admin <username 15>	Name of the admin account.
user <username 15>	Name of the user account.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create the admin-level user “dlink”:

```
DGS-3200-10:4#create account admin dlink
Command: create account admin dlink

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

DGS-3200-10:4#
```

To create the user-level user “System”:

```
DGS-3200-10:4##create account user System
Command: create account user System

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

DGS-3200-10:4#
```

4-2 enable password encryption

Purpose

To create user accounts.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable password encryption

```
DGS-3200-10:4#enable password encryption
Command: enable password encryption


Success.


DGS-3200-10:4#
```

4-3 disable password encryption

Purpose

To create user accounts.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable password encryption

```
DGS-3200-10:4#disable password encryption
Command: disable password encryption

Success.

DGS-3200-10:4#
```

4-4 config account

Purpose

To configure user accounts.

Format

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

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-I.

Parameters

Parameters	Description
<username>	Name of the account. The account must already be defined.
plain_text	Select to specify the password in plain text form.
sha_1	Select to specify the password in the SHA-I encrypted form.
password	The password for the user account. The length for of password in plain-text form and in encrypted form are

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

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the user password of “dlink” account :

```
DGS-3200-10:4#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-3200-10:4#
```

To configure the user password of “`adminstrator`” account :

```
 DGS-3200-10:4#config account adminstrator
 Command: config account administrator encrypt sha_1
*@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq
 Success.

 DGS-3200-10:4#
```

4-5 show account

Purpose

To display user accounts.

Format

show account

Description

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

Parameters

None.

Restrictions

None.

Example

To display the accounts that have been created:

```
DGS-3200-10:4#show account
Command: show account


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



DGS-3200-10:4#
```

4-6 delete account

Purpose

To delete an existing account.

Format

delete account <username>

Description

This command is used to delete an existing account.

Parameters

Parameters	Description
<username>	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-3200-10:4#delete account System
Command: delete account System

Success.

DGS-3200-10:4#
```

4-7 show session

Purpose

To display a list of currently logged-in users.

Format

show session

Description

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

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display a list of currently logged-in users:

```
DGS-3200-10:4# show session
Command: show session

ID  Live Time     From                         Level  Name
--  ------------  ---------------------------  -----  ---------------
8   23:37:42.270  Serial Port                   4     Anonymous

Total Entries: 1

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

4-8 show switch

Purpose

Used to display the switch information.

Format

show switch

Description

This command is used to display the switch information.

Parameters

None.

Restrictions

None.

Example

To display the switch information:

```
DGS-3200-10:4#show switch
Command: show switch

Device Type        : DGS-3200-10 Gigabit Ethernet Switch
MAC Address        : 00-00-00-01-02-00
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.B006
Firmware Version   : Build 1.35.B019
Hardware Version   : A2
Serial Number      : P4CK183000001
System Name        :
System Location    :
System Contact     :
Spanning Tree      : Disabled
GVRP               : Disabled
IGMP Snooping      : Disabled
MLD Snooping       : Disabled
Telnet             : Disabled (TCP 23)
```

```
Web                  : Enabled (TCP 80)
SNMP                 : Enabled
RMON                 : Disabled
SSL Status           : Disabled
SSH Status           : Disabled
802.1x               : Disabled
Jumbo Frame          : Off
CLI Paging           : Enabled
MAC Notification     : Disabled
Port Mirror          : Disabled
SNTP                 : Disabled
Syslog Global State   : Disabled
Single IP Management : Disabled
Dual Image              : Supported
Password Encryption Status  : Disabled
DGS-3200-10:4#
```

4-9 show environment

Purpose

To display the device internal temperature.

Format

show environment

Description

This command is used to display the device internal temperature status.

Parameters

None.

Restrictions

Only DGS-3200-16 supports this command. DGS-3200-10 does not support this command.

Example

To display the switch internal temperature status:

```
DGS-3200-16:4# show environment
Command: show environment

Side Fan                  Temperature
                           (Celsius)
--------                  -------------
   OK                          47

Note: The warning temperature is above 83 degrees.


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

4-10 show serial_port

Purpose

To display the current serial port setting.

Format

show serial_port

Description

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

Parameters

None.

Restrictions

None.

Example

To display the serial port setting:

```
DGS-3200-10:4#show serial_port
Command: show serial_port

Baud Rate      : 115,200
Data Bits      : 8
Parity Bits    : None
Stop Bits      : 1
Auto-Logout    : 10 mins

DGS-3200-10:4#
```

4-11 config serial_port

Purpose

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] }

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.

Parameters

Parameters	Description	
baud_rate	The serial bit rate that will be used to communicate with the management host. There are four options: **9600**, **19200**, **38400**, and **115200**.	
auto_logout	The auto logout time out setting :	
	never	Never timeout.
	2_minutes	When you idle over 2 minutes, the device will auto logout.
	5_minutes	When you idle over 5 minutes, the device will auto logout.
	10_minutes	When you idle over 10 minutes, the device will auto logout.
	15_minutes	When you idle over 15 minutes, the device will auto logout.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the baud rate:

```
DGS-3200-10:4# config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600


Success.


DGS-3200-10:4#
```

4-12 enable clipaging

Purpose

To pause the scrolling of the console screen when the show command displays more than one page.

Format

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.

Parameters

None.

Restrictions

Only Administrator-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-3200-10:4#enable clipaging
Command: enable clipaging


Success.


DGS-3200-10:4#
```

4-13 disable clipaging

Purpose

To disable pause the scrolling of the console screen when the show command displays more than one page.

Format

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.

Parameters

None.

Restrictions

Only Administrator-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-3200-10:4#disable clipaging
Command: disable clipaging


Success.


DGS-3200-10:4#
```

4-14 enable telnet

Purpose

The switch allows you manage the switch via Telnet based management software.

Use the command to enable Telnet and configure a port number.

Format

enable telnet {<tcp_port_number 1-65535>}

Description

This command is used to enable Telnet and configure the port number.

Parameters

Parameters	Description
tcp_port_number	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-level users can issue this command.

Example

To enable Telnet and configure a port number:

```
DGS-3200-10:4#enable telnet 23
Command: enable telnet 23


Success.


DGS-3200-10:4#
```

4-15 disable telnet

Purpose

To disable Telnet.

Format

disable telnet

Description

This command is used to disable Telnet.

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable Telnet:

```
DGS-3200-10:4#disable telnet
Command: disable telnet

Success.

DGS-3200-10:4#
```

4-16 enable web

Purpose

The switch can be managed via HTTP-based management software. Use this command to enable HTTP and configure the port number.

Format

enable web {<tcp_port_number 1-65535>}

Description

This command is used to enable HTTP and configure the port number.

Parameters

Parameters	Description
tcp_port_number	The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Web protocol is 80

Restrictions

Only Administrator-level users can issue this command.

Example

To enable HTTP and configure port number:

```
DGS-3200-10:4#enable web 80
Command: enable web 80

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

DGS-3200-10:4#
```

4-17 disable web

Purpose

To disable HTTP.

Format

disable web

Description

This command is used to disable HTTP.

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable HTTP :

```
DGS-3200-10:4#disable web
Command: disable web

Success.

DGS-3200-10:4#
```

4-18 save

Purpose

To save changes in non-volatile RAM.

Format

save{[config <config_id 1-2> | log | all]}

Description

The save command saves changes in non-volatile RAM.

Parameters

Parameters	Description
config <config_id 1-2>	Specifes the configuration identify number of the indicated configuration.
log	Save log.
all	Save changes to currently active configuration and save log
	If no any keyword specified, save changes to configuration

Restrictions

Only Administrator-level users can issue this command.

Example

To save changes to non-volatile RAM:

```
DGS-3200-10:4#save
Command: save


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


DGS-3200-10:4#
```

To save configuration 1 to NV-RAM:

```
DGS-3200-10:4#save config 1
Command: save config 1


Saving configuration 1 to NV-RAM.......... Done.


DGS-3200-10:4#
```

To save a log to NV-RAM:

```
DGS-3200-10:4#save log
Command: save log


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


DGS-3200-10:4#
```

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

```
DGS-3200-10:4#save all
Command: save all


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


DGS-3200-10:4#
```

4-19 reboot

Purpose

To restart the switch.

Format

reboot

Description

This command is used to restart the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To restart the switch:

```
DGS-3200-10:4#reboot
Command: reboot


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

4-20 reset

Purpose

To reset all switch parameters.

Format

reset {[config | system]}

Description

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

Parameter

Parameters	Description
config	If you specify the **config** keyword , all parameters are reset to default settings. But device will neither save nor reboot.
system	If you specify the **system** keyword, all parameters are reset to default settings. Then the switch will do factory reset, save, and reboot.
	If no keyword is specified , all parameters will be reset to default settings except IP address, user account, and history log. But 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-3200-10:4#reset
Command: reset


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


DGS-3200-10:4#
```

To reset the system configuration settings:

```
DGS-3200-10:4#reset config
Command: reset config

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

DGS-3200-10:4#
```

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

```
DGS-3200-10:4#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…
```

4-21 login

Purpose

To login to the switch.

Format

login

Description

This command is used to log in to the switch.

Parameter

None.

Restrictions

None.

Example

To login to the switch:

```
DGS-3200-10:4#login
Command: login

UserName:
```

4-22 logout

Purpose

Used to log out of the switch.

Format

logout

Description

This command is used to logout.

Parameter

None.

Restrictions

None.

Example

To logout of the switch:

```
DGS-3200-10:4#logout
Command: logout



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



                        DGS-3200-10 Gigabit Ethernet Switch
                               Command Line Interface

                             Firmware: Build 1.35.B019
             Copyright(C) 2009 D-Link Corporation. All rights reserved.
Username:
Password:
```

5 Utility Command List

```
download [ firmware_fromTFTP [ <ipaddr> | <ipv6addr> ] <path_filename 64> image_id <1-2> ]
| [ cfg_fromTFTP [ <ipaddr> | <ipv6addr> ] <path_filename 64> {[<config_id 1-2> | increment]} ]
upload log_toTFTP [ <ipaddr> | <ipv6addr> ] <path_filename 64> ]
upload cfg_toTFTP [ <ipaddr> | <ipv6addr> ] <path_filename 64> { <config_id 1-2>}
config firmware image_id <1-2> [delete | boot_up]
config configuration <config_id 1-2> [boot_up | delete | active]
show firmware information
show config [ current_config | config_in_nvram <config_id 1-2> | information ]
ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
ping6 <ipv6addr> {times <value 1-255>| size <value 1-6000> | timeout <value 1-10>}
traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe
<value 1-9>}
telnet <ipaddr> {tcp_port <value 0-65535>}
```

Note: The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 adress. The field may be omitted for global IPv6 addresses. For example,

```
DGS-3200-10:4#upload cfg_toTFTP fe80::20d:88ff:fe11:7b6c%System DGS-3200.cfg
```

5-1 download

Purpose

To download and install new firmware or a switch configuration file from a TFTP server.

Format

```
download [ firmware_fromTFTP [ <ipaddr> | <ipv6addr> ] <path_filename 64> image_id <1-2> ]
| [ cfg_fromTFTP [<ipaddr> | <ip6addr>] <path_filename 64> {[<config_id 1-2> | increment]} ]
```

Description

This command is used to download a new firmware or a switch configuration file from a TFTP server. The firmware can be loaded to different section according to the **image_id** or the **config_id**.

Parameters

Parameters	Description
firmware_fromTFTP	Download and install new firmware on the switch from a TFTP server.
cfg_fromTFTP	Download a switch configuration file from a TFTP server.
ipaddr	The IP address of the TFTP server.
ipv6addr	The IPv6 address of the TFTP server.
path_filename	The DOS path and filename of the firmware or switch configuration file on the TFTP server. The maximum length is 64.
image_id <1-2>	Specifes the image identify number of the indicated firmware.
config_id <1-2>	Specifes the configuration identify number of the indicated configuration.
increment	Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.

Restrictions

Only Administrator-level users can issue this command.

Examples

Download firmware:

```
DGS-3200-10:4#download firmware_fromTFTP 10.90.90.90 c:/DGS3200_Run_1_35_B019.had
Command: download firmware_fromTFTP 10.90.90.90 c:/DGS3200_Run_1_35_B019.had


Connecting to server.................. Done.
Download firmware..................... Done.   Do not power off !!
Please wait, programming flash......... Done.
Success


DGS-3200-10:4#
```

5-2 upload

Purpose

To upload the current switch settings or the switch history log to a TFTP server.

Format

upload log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>

upload cfg_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> { <config_id 1-2>}

Description

This command is used to upload either the switch's configuration or the switch's history log to a TFTP server.

Parameters

Parameters	Description
log_toTFTP	Specifies that the switch history log will be uploaded to the TFTP server.
cfg_toTFTP	Specifies that the switch configuration will be uploaded to the TFTP server.
ipaddr	The IP address of the TFTP server.
ipv6addr	The IPv6 address of the TFTP server.
path_filename	Specifies 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.
config_id <1-2>	Specifies the configuration identify number of the indicated configuration.

Restrictions

Only Administrator-level users can issue this command.

Examples

Upload configuration to TFTP server:

```
DGS-3200-10:4#upload cfg_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\cfg config_id 1
Command: upload cfg_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\cfg config_id 1


Connecting to server... Done.
Upload configuration... Done.


DGS-3200-10:4#
```

Upload system log to TFTP server:

```
DGS-3200-10:4#upload log_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\log
Command: upload log_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\log

Connecting to server... Done.
Upload configuration... Done.

DGS-3200-10:4#
```

5-3 config firmware

Purpose

To configure the specific firmware as boot up image or delete the specific firmware.

Format

config firmware image_id <1-2> [delete | boot_up]

Description

This command is used to configure firmware as a boot-up image or to delete the firmware.

Parameters

Parameters	Description
image_id <1-2>	Specifes the serial number of the indicated firmware.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete the specific firmware:

```
DGS-3200-10:4#config firmware image_id 2 delete
Command: config firmware image_id 2 delete

Are you sure you want to delete firmware image_id 1?(y/n) y
Success.

DGS-3200-10:4#
```

To configure the specific firmware as boot up image:

```
DGS-3200-10:4#config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up


Success!


DGS-3200-10:4#
```

5-4 config configuration

Purpose

To configure the specific configuration, boot up or active, or to delete it.

Format

config configuration <config_id 1-2> [boot_up | delete | active]

Description

This command is used to configure the specific configuration, boot up or active, or to delete it.

Parameters

Parameters	Description
config_id <1-2>	Specifes the serial number of the indicated configuration.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete the specific configuration:

```
DGS-3200-10:4#config configuration config_id 2 delete
Command: config configuration config_id 2 delete


Success


DGS-3200-10:4#
```

5-5 show firmware information

Purpose

To display firmware information.

Format

show firmware information

Description

This command is used to display firmware information.

Parameters

None

Restrictions

Only Administrator-level users can issue this command.

Example

To display firmware information:

```
DGS-3200-10:4#show firmware information
Command: show firmware information

Image ID        : 1(Boot up firmware)
    Version     : 1.35.B019
    Size         : 2075194 Bytes
    Update Time: 2000/01/01 00:57:40
    From         : 172.18.211.108(Console)
    User         : Anonymous


Image ID   : 2
    Version     : (Empty)
    Size         :
    Update Time:
    From         :

DGS-3200-10:4#
```

5-6 show config information

Purpose

To display the configuration or configuration information.

Format

show config [current_config | config_in_nvram <config_id 1-2> | information]

Description

This command is used to display configuration information.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display configuration information:

```
DGS-3200-10:4#show config information
Command: show config information

ID            : 1(Boot up configuration)
 ------------- ------------- ----------------------------
 Version      : 1.35.B019
 Size         : 10595 Bytes
 Updata Time : 2000/01/01 00:32:25
 From         : FE80::21A:4DFF:FE32:EFB9(Console)
 User         : Anonymous
 Boot Up      : Yes


 ID            : 2
 ------------- ------------- ----------------------------
 Version       : 1.35.B019
 Size          : 10102 Bytes
 Updata Time   : 2000/01/01 00:02:40
 From          : Local save(Console)
 User          : Anonymous
 Boot Up       : No

DGS-3200-10:4#
```

5-7 ping

Purpose

To test the connectivity between network devices.

Format

ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}

Description

This command sends 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.

Parameters

Parameters	Description
ipaddr	Specify the IP address of the host.
value	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 value is 0.
sec	Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.

Restrictions

Only Administrator-level users can issue this command.

Example

To send ICMP echo message to “10.51.17.1” for 4 times:

```
DGS-3200-10:4#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-3200-10:4#
```

5-8 ping6

Purpose

To test the connectivity between network devices.

Format

ping6 <ip6addr> {times <value 1-255> | size <value 1-6000> | timeout <value 1-10>}

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.

Parameters

Parameters	Description
ip6addr	Specify the IPv6 address of the host.
times	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.
size	Defines the size. A value of 1 to 6000 can be specified.
timeout	Defines the time-out period while waiting for a response from the remote device. A value of 1 to 10 can be specified.

Restrictions

Only Administrator-level users can issue this command.

Example

To send ICMP echo message to "3FFE:2::D04D:7878:66D:E5BC" for 10 times:

```
DGS-3200-10:4#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-3200-10:4#
```

5-9 traceroute

Purpose

To trace the routed path between the switch and a destination endstation.

Format

traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}

Description

This command is used to trace a route between the switch and a give host on the network.

Parameters

Parameters	Description
ipaddr	IP address of the destination endstation.
ttl <value1-60>	The time to live value of the trace route request. This is the maximum number of routers The traceroute command will cross while seeking the network path between two devices.
port<value 30000-64900>	The port number. Must be above 1024. The value range is from 30000 to 64900 .
probe<value 1-9>	The number of probes. The range is from 1 to 9 .

Restrictions

Only Administrator-level users can issue this command.

Example

To trace the routed path between the switch and 10.48.74.121:

```
DGS-3200-10:4#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3


1   <10 ms.     10.48.74.121
1   <10 ms.     10.48.74.121
1   <10 ms.     10.48.74.121


DGS-3200-10:4#
```

5-10 telnet

Purpose

To login a host that supports Telnet.

Format

telnet <ipaddr> {tcp_port <value 0-65535>}

Description

This command is used to login a host that supports Telnet.

Parameters

Parameters	Description
ipaddr	The IP address of the host to login.
tcp_port	The Telnet port.

Restrictions

None.

Example

To Telnet to a host:

```
DGS-3200-10:4#telnet 10.1.1.1
Command: telnet 10.1.1.1

 Connecting to 10.1.1.1...
[Press Ctrl+Y to disconnect.]

DGS-3200-10:4#Welcome to Microsoft Telnet Service

login: administrator
password:

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\Administrator>exit
Connection to host lost.

DGS-3200-10:4#
```

Note: Use “Ctrl+Y” to connect from the host.

6 Power Saving Command List

config power_saving state [enable|disable]
show power_saving

6-1 config power_saving

Purpose

To configure power saving.

Format

config power_saving state [enable|disable]

Description

This command is used to configure the power saving for the system.

Parameters

Parameters	Description
state	Configure the power saving state to enable or disable.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure power saving:

```
DGS-3200-10:4# config power_saving state enable
Command: config power_saving state enable


Success


DGS-3200-10:4#
```

6-2 show power_saving

Purpose

To show power saving information.

Format

show power_saving

Description

This command is used to display power saving information.

Parameters

None.

Restrictions

None.

Examples

To display power saving information:

```
DGS-3200-10:4#show power_saving
Command: show power_saving


Power Saving State:     Enabled



DGS-3200-10:4#
```

IV. Network Management

The Fundamentals section includes the following chapters: SNMPv1/v2, SNMPv3, Network Management, Network Monitoring, System Severity, Command List History, Modify Banner and Prompt, Time and SNTP, Jumbo Frame, Single IP Management, and Safeguard Engine.

7 SNMPv1/v2 Command List

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community <community_string 32>
show snmp community <community_string 32>

Note: If SNMPv3 commands are used, the SNMPv1/v2 commands are not necessary.

7-1 create snmp community

Purpose

To create an SNMP community string.

Format

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

Description

This command is used to create an SNMP community string and to specify the string as enabling read only or read-write privileges for the SNMP management host.

Parameters

Parameters	Description
community_string	An alphanumeric string of up to 32 characters used in the authentication of users wanting access to the switch's SNMP agent.
view	An alphanumeric string of up to 32 characters.
read_only	Allows the user using the above community string to have read-only access to the switch's SNMP agent. The default read-only community string is public.
read_write	Allows the user using the above community string to have read and write acces to the switch's SNMP agent. The default read-write community string is private.

Restrictions

Only Administrator-level users can issue this command. A maximum of four community strings can be specified.

Example

To create a read-only level SNMP community "System":

```
DGS-3200-10:4# create snmp community System view CommunityView read_write
Command: create snmp community System view CommunityView read_write

Success.

DGS-3200-10:4#
```

7-2 delete snmp community

Purpose

To delete an SNMP community string previously entered on the switch.

Format

delete snmp community <community_string 32>

Description

This command is used to delete an SNMP community string entered on the switch using the create snmp community command above.

Parameters

Parameters	Description
community_string	An alphanumeric string of up to 32 characters used in the authentication of users wanting access to the switch's SNMP agent.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a read-only level SNMP community "System":

```
DGS-3200-10:4#delete snmp community System
Command: delete snmp community System

Success.

DGS-3200-10:4#
```

7-3 show snmp community

Purpose

To display the SNMP community configurations on the switch.

Format

show snmp community <community_string 32>

Description

This command is used to display the following information: SNMP community strings, View Name, and Access Rights.

Parameter

Parameters	Description
community_string	An alphanumeric string of up to 32 characters used in the authentication of users wanting access to the switch's SNMP agent.

Restrictions

None.

Example

To display SNMP community information:

```
DGS-3200-10:4#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-3200-10:4#
```

8 SNMPv3 Command List

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> }
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>}
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> }
show snmp traps

Note: If SNMPv3 commands are used, SNMPv1/v2 commands are not necessary.

8-1 create snmp user

Purpose

To create a new user to an SNMP group originated by this command.

Format

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > | sha <auth_password 8-20 >] priv [none | des <priv_password 8-16>]| by_key auth [md5 <auth_key 32-32>| sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

Description

This command is used to create a new user to an SNMP group originated by this command. Users can chose input authencation and privacy by password or by key.

Parameters

<table>
<tr><th>Parameters</th><th colspan="2">Description</th></tr>
<tr><td><b>user_name</b></td><td colspan="2">The name of the user on the host that connects to the agent.
The range is 1 to 32 .</td></tr>
<tr><td><b>groupname</b></td><td colspan="2">The name of the group to which the user is associated.
The range is 1 to 32 .</td></tr>
<tr><td><b>encrypted</b></td><td colspan="2">Specifies whether the password appears in encrypted format.</td></tr>
<tr><td><b>by_password</b></td><td colspan="2">indicate input password for authentication and privacy</td></tr>
<tr><td><b>by_key</b></td><td colspan="2">indicate input key for authentication and privacy</td></tr>
<tr><td rowspan="3"><b>auth</b></td><td colspan="2">Initiates an authentication level setting session.
The options are md5 and sha .</td></tr>
<tr><td><b>md5</b></td><td>The HMAC-MD5-96 authentication level.</td></tr>
<tr><td><b>sha</b></td><td>The HMAC-SHA-96 authentication level.</td></tr>
<tr><td><b>auth_password</b></td><td colspan="2">A authentication string used by MD5 or SHA1.</td></tr>
<tr><td><b>priv_password</b></td><td colspan="2">A privacy string used by DES.</td></tr>
<tr><td><b>auth_key</b></td><td colspan="2">A authentication key used by MD5 or SHA1, it is hex string type.</td></tr>
<tr><td><b>priv_key</b></td><td colspan="2">A privacy key used by DES, it is hex string type.</td></tr>
</table>

Restrictions

Only Administrator-level users can issue this command.

Example

To create a new user to an SNMP group originated by this command:

```
DGS-3200-10:4#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 1234
5678 priv des 12345678

Success.

DGS-3200-10:4#
```

8-2 delete snmp user

Purpose

To remove a user from an SNMP group and delete the associated group in SNMP group.

Format

delete snmp user <user_name 32>

Description

This command is used to remove a user from an SNMP group and deletes the associated group in the SNMP group.

Parameters

Parameters	Description
username	The name of the user on the host that connects to the agent. The range is 1 to 32 .

Restrictions

Only Administrator-level users can issue this command.

Example

To delete an SNMP user:

```
DGS-3200-10:4#delete snmp user dlink
Command: delete snmp user dlink


Success.


DGS-3200-10:4#
```

8-3 show snmp user

Purpose

To display information on each SNMP username in the group username table.

Format

show snmp user

Description

This command is used to display information on each SNMP username in the group username table.

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display SNMP user information:

```
DGS-3200-10:4#show snmp user
Command: show snmp user

Username                          Group Name                        VerAuthPriv
---------------------------  ---------------------------  ------------
initial                           initial                            V3 NoneNone

Total Entries : 1

DGS-3200-10:4#
```

8-4 show snmp groups

Purpose

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

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the names of the SNMP groups on the switch:

```
DGS-3200-10:4#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv2
Securiy Level    : NoAuthNoPriv

Group    Name    : initial
ReadView Name    : restricted
WriteView Name   :
Notify View Name : restricted
Securiy Model    : SNMPv3
Securiy Level    : NoAuthNoPriv

Group    Name    : private
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : private
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv2
Security Level   : NoAuthNoPriv

Group    Name    : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv2
Security Level   : NoAuthNoPriv

Group    Name    : WriteGroup
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : WriteGroup
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : WriteGroup
```

```
ReadView Name     : CommunityView
WriteView Name    : CommunityView
Notify View Name  : CommunityView
Security Model    : SNMPv2
Security Level    : NoAuthNoPriv

Group    Name     : D-Link_group
ReadView Name     : CommunityView
WriteView Name    : CommunityView
Notify View Name  : CommunityView
Security Model    : SNMPv3
Security Level    : authPriv

Total Entries: 10

DGS-3200-10:4
```

8-5 create snmp view

Purpose

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]

Description

This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.

Parameters

Parameters	Description	
view_name	View name to be created.	
oid	Object-Identified tree, MIB tree.	
view_type	Specify the access type of of the MIB tree in this view .	
	included	Includes this view.
	excluded	Excludes 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-3200-10:4#create snmp view dlinkview 1.3.6 view_type included

Command: create snmp view dlinkview 1.3.6 view_type included


Success.


DGS-3200-10:4#
```

8-6 delete snmp view

Purpose

To remove a view record.

Format

delete snmp view <view_name 32> [all | <oid>]

Description

This command is used to remove a view record.

Parameters

Parameters	Description
view_name	View nameof the user who will be deleted.
all	All view records.
oid	Object-Identified tree, MIB tree.

Restrictions

Only Administrator-level users can issue this command.

Example

To remove a view record:

```
DGS-3200-10:4#delete snmp view dlinkview all

Command: delete snmp view dlinkview all


Success.


DGS-3200-10:4#
```

8-7 show snmp view

Purpose

To display SNMP view records.

Format

show snmp view {<view_name 32>}

Description

This command is used to display SNMP view records.

Parameters

Parameters	Description
view_name	View name of the user who likes to show.

Restrictions

Only Administrator-level users can issue this command.

Example

To display SNMP view records:

```
DGS-3200-10:4#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-3200-10:4#
```

8-8 create snmp community

Purpose

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. You can specify one or more of the following characteristics associated with the string:

An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.

A MIB view, which defines the subset of all MIB objects accessible to the given community.
Read and write or read-only permission for the MIB objects accessible to the community.

Format

create snmp community <community_string 32> view <view_name 32> [read_only|read_write]

Description

This command is used to create an SNMP community string.

Parameters

Parameters	Description
community_string	Communtiy string. Max string length is 32.
view_name	View name. A MIB view. Max length is 32
[read_only | read_write]	Read and write or read-only permission.

Restrictions

Only Administrator-level users can issue this command.

Example

To create an SNMP community string:

```
DGS-3200-10:4#create snmp community dlink view CommunityView read_write
Command: create snmp community dlink view CommunityView read_write


Success.


DGS-3200-10:4#
```

8-9 delete snmp community

Purpose

To remove a specific communtiy string

Format

delete snmp community <community_string 32>

Description

This command is used to remove a specific community string.

Parameters

Parameters	Description
community_string 32	The community string that will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete an SNMP community:

```
DGS-3200-10:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3200-10:4#
```

8-10 show snmp community

Purpose

To display community string configurations

Format

show snmp community { <community_string 32> }

Description

This command is used to display community string configurations..

Parameters

Parameters	Description
community_string 32	The community string to be displayed.
	If a community string is not specified, all community string information will be displayed.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the current community string configurations:

```
 DGS-3200-10:4#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-3200-10:4#
```

8-11 config snmp engineID

Purpose

To configure an identifier for the SNMP engine on the switch.

Format

config snmp engineID <snmp_engineID 10-64>

Description

This command is used to configure an identifier for the SNMP engine on the switch. Associated with each SNMP entity is a unique engineID.

Parameters

Parameters	Description
snmp_engineID	Identify for the SNMP engine on the switch. It is an octet string type.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure an identifier for the SNMP engine on the switch:

```
DGS-3200-10:4#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DGS-3200-10:4#
```

8-12 show snmp engineID

Purpose

To display the identification of the SNMP engine on the switch.

Format

show snmp engineID

Description

This command is used to display the identification of the SNMP engine on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the identification of an SNMP engine:

```
DGS-3200-10:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DGS-3200-10:4#
```

8-13 create snmp group

Purpose

To create a new SNMP group, or a table that maps SNMP users to SNMP views

Format

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

Description

This command is used to create a new SNMP group.

Parameters

Parameters	Description	
groupname	The name of the group.	
v1	The least secure of the possible security models.	
v2c	The second least secure of the possible security models.	
v3	The most secure of the possible security models. Specifies authentication of a packet.	
	noauth_nopriv	neither support packet authentication nor encrypting.
	auth_nopriv	Support packet authentication .
	auth_priv	Support packet authentication and encrypting.
view_name	View name. A MIB view.	

Restrictions

Only Administrator-level users can issue this command.

Example

To create a new SNMP group:

```
DGS-3200-10:4#create snmp group D-Link_group v3 auth_priv read_view CommunityView
write_view CommunityView notify_view CommunityView
Command: create snmp group D-Link_group v3 auth_priv read_view CommunityView wri
te_view CommunityView notify_view CommunityView

Success.

DGS-3200-10:4#
```

8-14 delete snmp group

Purpose

To remove an SNMP group.

Format

delete snmp group <groupname 32>

Description

This command is used to remove an SNMP group.

Parameters

Parameters	Description
groupname	The name of the group will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Example

To remove an SNMP group:

```
DGS-3200-10:4#delete snmp group D_Link_group
Command: delete snmp group D_Link_group


Success.


DGS-3200-10:4#
```

8-15 create snmp host

Purpose

To create a recipient of an SNMP trap operation.

Format

create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>

Description

This command is used to create a recipient of an SNMP operation.

Parameters

Parameters	Description
ipaddr	The IP address of the recipient for which the traps are targeted.
v6host	Specifies the v6host IP address to which the trap packet will be sent.
v1	The least secure of the possible security models.
v2c	The second least secure of the possible security models.
v3	The most secure of the possible.

	noauth_nopriv	neither support packet authentication nor encrypting.
	auth_nopriv	Support packet authentication .
	auth_priv	Support packet authentication and encrypting.
auth_string	The authentication string.	

Restrictions

Only Administrator-level users can issue this command.

Example

To create a recipient of an SNMP operation:

```
DGS-3200-10:4#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-3200-10:4#
```

8-16 delete snmp host

Purpose

To delete a recipient of an SNMP trap operation.

Format

delete snmp [host <ipaddr> | v6host <ipv6addr>]

Description

This command is used to delete a recipient of an SNMP trap operation.

Parameters

Parameters	Description
ipaddr	The IP address of the recipient for which the traps are targeted.
v6host	Specifies the v6host IP address.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a recipient of an SNMP trap operation:

```
DGS-3200-10:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DGS-3200-10:4#
```

8-17 show snmp host

Purpose

To display the recipient for which the traps are targeted.

Format

show snmp host { <ipaddr> }

Description

This command is used to display the recipient for which the traps are targeted.

Parameters

Parameters	Description
ipaddr	The IP address of the recipient for which the traps are targeted.
	If no parameter specified, all SNMP hosps will be diplayed.
v6host	Specifies the v6host IP address.

Restrictions

None.

Example

To display the receipient for which the traps are targeted:

```
DGS-3200-10:4# 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-3200-10:4#
```

8-18 show snmp v6host

Purpose

To display the recipient for which the traps are targeted.

Format

show snmp v6host { <ipv6addr> }

Description

This command is used to display the recipient for which the traps are targeted.

Parameters

Parameters	Description
ipaddr	The IP address of the recipient for which the traps are targeted.
	If no parameters are specified, all SNMP hosts will be displayed.
v6host	Specifies the v6host IP address.

Restrictions

None.

Example

To display the recipient for which the traps are targeted:

```
DGS-3200-10:4# 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: 123456789101234567890

Host IPv6 Address: FECO:1A49:2AA:FF:FE34:CA8F
SNMP Version      : V3 a/np
Community Name/SNMPv3 User Name: abcdefghijk

Total Entries : 2

DGS-3200-10:4#
```

8-19 show snmp traps

Purpose

To display the status of SNMP trap and authentication traps.

Format

show snmp traps

Description

This command is used to show the trap state.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the SNMP trap and authentication trap status:

```
DGS-3200-10:4#show snmp traps
Command: show snmp traps

SNMP Traps          : Enabled
Authenticate Trap   : Enabled

DGS-3200-10:4#
```

9 Network Management Command List

enable snmp

disable snmp

create trusted_host [<ipaddr> | network <network_address>]

delete trusted_host [ipaddr <ipaddr> | network <network_address>| all]

show trusted_host {<ipaddr>}

config snmp system_name {<sw_name>}

config snmp system_location {<sw_location>}

config snmp system_contact {<sw_contact>}

enable rmon

disable rmon

enable snmp traps

disable snmp traps

enable snmp authenticate_traps

disable snmp authenticate_traps

9-1 enable snmp

Purpose

To enable the SNMP interface access function.

Format

enable snmp

Description

This command is used to enable the SNMP function. When SNMP function is disabled, the network manager will not be able the access SNMP MIB objects. The device will not send traps or notification to network manager either.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNMP:

```
DGS-3200-10:4#enable snmp
Command: enable snmp

Success.

DGS-3200-10:4#
```

9-2 disable snmp

Purpose

To disable the SNMP interface access function.

Format

disable snmp

Description

This command is used to disable the SNMP function. When SNMP function is disabled, the network manager will not be able the access SNMP MIB objects. The device will not send traps or notification to network manager either.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SNMP:

```
DGS-3200-10:4#disable snmp
Command: disable snmp

Success.

DGS-3200-10:4#
```

9-3 create trusted_host

Purpose

To create the trusted host.

Format

create trusted_host [<ipaddr> | network <network_address>]

Description

This command is used to create the trusted host. The switch allows you to specify up to ten IP addresses that are allowed to manage the switch via in-band SNMP or Telnet based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the switch, provided the user knows the Username and Password.

Parameters

Parameters	Description
ipaddr	The IP address of the trusted host.
network	The network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a trusted host:

```
DGS-3200-10:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121


Success.


DGS-3200-10:4#
```

9-4 delete trusted_host

Purpose

To delete a trusted host entry made using the **create trusted_host** command above.

Format

delete trusted_host [ipaddr <ipaddr> | all]

Description

This command is used to delete a trusted host entry made using the **create trusted_host** command above.

Parameters

Parameters	Description
ipaddr <all>	The IP address of the trusted host
network	The network address of the trusted network.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a trusted host:

```
DGS-3200-10:4#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121


Success.


DGS-3200-10:4#
```

9-5 show trusted_host

Purpose

To display a list of trusted hosts entered on the switch using the **create trusted_host** command above.

Format

show trusted_host {<ipaddr>}

Description

This command is used to display the trusted hosts.

Parameters

None.

Restrictions

None.

Example

To display a trusted host:

```
DGS-3200-10:4#show trusted_host
Command: show trusted_host

Management Stations

IP Addrress
---------------
10.48.93.100
10.51.17.1
10.50.95.90

Total Entries : 3

DGS-3200-10:4#
```

9-6 config snmp system_name

Purpose

To configure the name for the switch.

Format

config snmp system_name {<sw_name>}

Description

This command is used to configure the name of the switch.

Parameter

Parameters	Description
sw_name	A maximum of 255 characters is allowed. A null string is also accepted.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the switch name for "`DGS-3200-10 Gigabit Ethernet Switch`":

.

```
DGS-3200-10:4# config snmp system_name DGS-3200-10 Gigabit Ethernet Switch
Command: config snmp system_name DGS-3200-10 Gigabit Ethernet Switch

Success.

DGS-3200-10:4#
```

9-7 config snmp system_location

Purpose

To enter a description of the location of the switch.

Format

config snmp system_location {<sw_location>}

Description

This command is used to enter a description of the location of the switch. A maximum of 255 characters can be used.

Parameter

Parameters	Description
sw_location	A maximum of 255 characters is allowed. A null string is also accepted.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the switch location for “HQ 5F”:

```
DGS-3200-10:4# config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3200-10:4#
```

9-8 config snmp system_contact

Purpose

To enter the name of a contact person who is responsible for the switch.

Format

config snmp system_contact {<sw_contact>}

Description

This command is used to enter the name and/or other information to identify a contact person who is responsible for the switch. A maximum of 255 characters can be used.

Parameters

Parameters	Description
sw_contact	A maximum of 255 characters is allowed. A null string is also accepted.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the switch contact to "MIS Department IV":

.

```
DGS-3200-10:4#config snmp system_contact "MIS Department IV"
Command: config snmp system_contact "MIS Department IV"

Success.

DGS-3200-10:4#
```

9-9 enable rmon

Purpose

To enable RMON on the switch.

Format

enable rmon

Description

This command is used to enable RMON on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable RMON on the switch:

```
DGS-3200-10:4#enable rmon
Command: enable rmon

Success.

DGS-3200-10:4#
```

9-10 disable rmon

Purpose

To disable RMON on the switch.

Format

disable rmon

Description

This command is used to disable RMON on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable RMON on the switch:

```
DGS-3200-10:4#disable rmon
Command: disable rmon

Success.

DGS-3200-10:4#
```

9-11 enable snmp traps

Purpose

To enable SNMP trap support.

Format

enable snmp traps

Description

This command is used to enable SNMP trap support on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNMP trap support:

```
DGS-3200-10:4#enable snmp traps
Command: enable snmp traps


Success.


DGS-3200-10:4#
```

9-12 disable snmp traps

Purpose

To disable SNMP trap support on the switch.

Format

disable snmp traps

Description

This command is used to disable SNMP trap support on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To prevent SNMP traps from being sent from the switch:

```
DGS-3200-10:4#disable snmp traps
Command: disable snmp traps


Success.


DGS-3200-10:4#
```

9-13 enable snmp authenticate_traps

Purpose

To enable SNMP authentication failure trap support.

Format

enable snmp authenticate_traps

Description

This command is used to enable SNMP authentication failure trap support.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNMP authentication trap support:

```
DGS-3200-10:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps


Success.


DGS-3200-10:4#
```

9-14 disable snmp authenticate_traps

Purpose

To disable SNMP authentication failure trap support.

Format

disable snmp authenticate_traps

Description

This command is used to disable SNMP authentication failure trap support.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SNMP authentication trap support:

```
DGS-3200-10:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps


Success.


DGS-3200-10:4#
```

10 Network Monitoring Command List

show packet ports <portlist>
show error ports <portlist>
show utilization [ports | cpu]
clear counters {ports <portlist> }
clear log
show log {index <value_list> }
enable syslog
disable syslog
show syslog
config syslog host [all|<index 1-4>] { severity [informational |warning |all] | **facility [local0|local1|local2|local3|local4|local5|local6|local7] |** **udp_port <udp_port_numer> |** **ipaddress <ipaddr> |** **state [enable|disable]}**
create syslog host <index 1-4> {severity [informational|warning|all] | facility[local0|local1 **|local2|local3|local4|local5|local6|local7] |udp_port <udp_port_number> | ipaddress <ipaddr>** **| state [enable|disable]}**
delete syslog host [<index 1-4> | all]
show syslog host {<index 1-4>}
config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]
show log_save_timing

10-1 show packet ports

Purpose

To display statistics about the packets sent and received by the switch.

Format

show packet ports <portlist>

Description

This command is used to display statistics about the packets sent and received by the switch.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the packets analysis for port 7:

```
DGS-3200-10:4#show packet ports 7
Command: show packet ports 7

Port number : 7
==============================================================================
Frame Size/Type  Frame Counts          Frames/sec
---------------  --------------------  --------------------
64                572                   27
65-127            151                   5
128-255           39                    0
256-511           65                    0
512-1023          7                     0
1024-1518         0                     0
Unicast RX        4                     0
Multicast RX      162                   1
Broadcast RX      568                   31

Frame Type        Total                 Total/sec
----------        --------------------  --------------------
RX Bytes          81207                 2237
RX Frames         734                   32
TX Bytes          8432                  0
TX Frames         100                   0
DGS-3200-10
```

10-2 show error ports

Purpose

To display the error statistics for a range of ports.

Format

show errors ports <portlist>

Description

This command is used to display error statistics for a range of ports.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the errors of port 3:

```
DGS-3200-10:4#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
```

10-3 show utilization

Purpose

To display real-time port utilization statistics.

Format

show utilization [ports | cpu]

Description

This command is used to display real-time port utilization or CPU statistics.

Parameters

None.

Restrictions

None.

Example

To display port utilization:

```
DGS-3200-10:4# show utilization ports
Command: show utilization ports


Port    TX/sec      RX/sec      Util
------  ----------  ----------  ----
 1      0           0           0
 2      0           0           0
 3      0           0           0
 4      0           0           0
 5      0           0           0
 6      0           0           0
 7      0           0           0
 8      0           0           0
```

To display CPU utilization:

```
DGS-3200-10:4# 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
```

10-4 clear counters

Purpose

To clear the switch’s statistics counters.

Format

clear counters {ports <portlist>}

Description

This command is used to clear the switch's statistics counters.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured. The beginning and end of the port list range are separated by a dash.
	If no parameter is specified, the system will count all of the ports.

Restrictions

Only Administrator-level users can issue this command.

Example

To clear the switch's statistics counters for ports 7 to 9:

```
DGS-3200-10:4#clear counters ports 7-9
Command: clear counters ports 7-9


Success.


DGS-3200-10:4#
```

10-5 clear log

Purpose

To clear the switch's history log.

Format

clear log

Description

This command is used to clear the switch's history log.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear the switch's history log:

```
DGS-3200-10:4#clear log
Command: clear log

Success

DGS-3200-10:4#
```

10-6 show log

Purpose

To display the switch history log.

Format

show log {index <value_list> }

Description

This command is used to display the switch history log.

Parameters

Parameters	Description
value_list	The **show log** command will display the history log between two values. For example, **show log index 1-5** will display the history log from 1 to 5.
	If no parameter is specified, all history log entries will be displayed.

Restrictions

None.

Examples

To display the switch history log:

```
DGS-3200-10:4#show log index 1-5
Command: show log index 1-5

Index  Date       Time       Log Text
-----  -------------------  ---------------------------------------------------
5      2000-01-01 00:00:41  Port 5 link down
4      2000-01-01 00:00:31  Port 3 link up, 100Mbps FULL duplex
3      2000-01-01 00:00:31  Successful login through Console (Username:Anonymous)
2      2000-01-01 00:00:31  Console session timed out (Username: dlink)
1      2000-01-01 00:00:31  Spanning Tree Protocol is disabled

DGS-3200-10:4#
```

10-7 enable syslog

Purpose

To enable syslog to send a message.

Format

enable syslog

Description

This command is used to enable syslog to send a message.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable syslog to send a message:

```
DGS-3200-10:4#enable syslog
Command: enable syslog


Success
DGS-3200-10:4#
```

10-8 disable syslog

Purpose

To disable syslog from sending a message.

Format

disable syslog

Description

This command is used to disable syslog from sending a message.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable syslog sending a message:

```
DGS-3200-10:4#disable syslog
Command: disable syslog

Success

DGS-3200-10:4#
```

10-9 show syslog

Purpose

To display the syslog protocol global state.

Format

show syslog

Description

This command is usded to display the syslog protocol global state.

Parameters

None.

Restrictions

None.

Examples

To display the syslog protocol global state:

```
DGS-3200-10:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3200-10:4#
```

10-10 config syslog host

Purpose

To configure the syslog host configuration.

Format

config syslog host [all |<index 1-4>] { severity [informational |warning | all] |

facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] |
udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable |disable]}

Description

This command is used to configure the syslog host configuration

Parameters

Parameters	Description	
host [all|<index 1-4>]	The host index or all hosts.	
severity	Three levels of support:	
	informational	informational messages
	warning	warning conditions
	all	any condition
facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the"local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values the switch supports now.	
	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	The UDP port number.	
ipaddr	The IP address of the host.	
state	The Ssyslog 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.	

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the syslog host configuration:

```
DGS-3200-10:4#config syslog host all severiry all facility local0
Command: config syslog host all severiry all facility local0


Success.


DGS-3200-10:4#
```

10-11 create syslog host

Purpose

To create a new syslog host.

Format

create syslog host <index 1-4> {severity [informational|warning|all] | facility[local0|local1 |local2|local3|local4|local5|local6|local7] |udp_port <udp_port_number> | ipaddress <ipaddr> |state [enable|disable]}

Description

This command is used to create a new syslog host.

Parameters

Parameters	Description	
host <index 1-4>	The host index.	
severity	Three levels are supported:	
	informational	Informational messages.
	warning	Warning conditions.
	all	Any condition.
facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the"local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values the switch supports now.	
	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	The UDP port number.	
ipaddr	The IP address of the host.	
state	The syslog protocol has been used for the transmission of event notification messages across networks to host. The option enables or disables the host to receive such messages.	

Restrictions

Only Administrator-level users can issue this command.

Example

To create a new syslog host:

```
DGS-3200-10:4#create syslog host 1 severity all facility local0
Command: create syslog host 1 severity all facility local0


Success.


DGS-3200-10:4#
```

10-12 delete syslog host

Purpose

To delete syslog host(s).

Format

delete syslog host [<index 1-4> | all]

Description

This command is used to delete syslog host(s).

Parameters

Parameters	Description
host [<index 1-4> | all]	Host index or all hosts.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a syslog host:

```
DGS-3200-10:4#delete syslog host 4
Command: delete syslog host 4


Success


DGS-3200-10:4#
```

10-13 show syslog host

Purpose

To display syslog host configurations.

Format

show syslog host {<index 1-4>}

Description

This command is used to display syslog host configurations.

Parameters

Parameters	Description
index	The host index.
	If no parameter is specified, all hosts will be displayed .

Restrictions

None.

Example

To display syslog host configurations:

```
DGS-3200-10:4#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host Id  Host IP Address  Severity        Facility  UDP port  Status
-------  ---------------  --------------  --------  --------  --------
1        10.1.1.2         All             Local0    514       Disabled
2        10.40.2.3        All             Local0    514       Disabled
3        10.21.13.1       All             Local0    514       Disabled

Total Entries : 3

DGS-3200-10:4#
```

10-14 config log_save_timing

Purpose

To configure the method to save log.

Format

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

Description

This command is used to set the method to save log.

Parameters

Parameters	Description
time_interval	Save log to flash every xxx minutes. (if no log happen in this period, don't save)
on_demand	Save log to flash whener user type "**save log**" or "**save all**".
log_trigger	Save log to flash whenever log arrives.

Restrictions

Only Administrator-level users can issue this command.

Notes

The default method is **on_demand**.

Examples

To configure method to save log as on demand:

```
DGS-3200-10:4# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DGS-3200-10:4#
```

10-15 show log_save_timing

Purpose

To show the method to save log.

Format

show log_save_timing

Description

This command is used to display the method to save log.

Parameters

None.

Restrictions

None.

Example

To show the timing method of the log save:

```
DGS-3200-10:4#show log_save_timing
Command: show log_save_timing

Saving log method: on_demand

DGS-3200-10:4#
```

11 System Severity Command List

config system_severity [trap | log | all] [critical | warning | information]

show system_severity

11-1 config system_severity

Purpose

To configure severity level control for the system.

Format

config system_severity [trap | log | all] [critical | warning | information]

Description

This command is used to configure severity level control for the system.

Parameters

Parameters	Description
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.
critical	Severity level = critical.
warning	Severity level = warning.
information	Severity level = information.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure severity level control for information level for a trap:

```
DGS-3200-10:4#config system_severity trap information
Command: config system_severity trap information


Success.


DGS-3200-10:4#
```

11-2 show system_severity

Purpose

To show the severity level control for a system.

Format

show system_severity

Description

This command is used to show the severity level control for a system.

Parameters

None.

Restrictions

None.

Examples

To show the severity level control for a system:

```
DGS-3200-10:4#
Command: show system_severity


System Severity Trap : warning
System Severity Log  : information


DGS-3200-10:4#
```

12 Command List History Command List

?

show command_history

dir

config command_history <value 1-40>

12-1 ?

Purpose

To display all the commands in the Command Line Interface (CLI).

Format

? {command}

Description

This command is used to display all of the commands available through the Command Line Interface (CLI).

Parameters

Parameters	Description
command	Specifies the command.
	If no command specified, the system will display all commands.

Restrictions

None.

Example

To display all commands:

```
DGS-3200-10:4# ?
Command: ?


..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear fdb
clear igmp_snooping data_driven_group
clear log
clear mac_based_access_control auth_mac
clear port_security_entry port
clear wac auth_state
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

12-2 show command_history

Purpose

To display the command history.

Format

show command_history

Description

This command is used to display the command history.

Parameters

None.

Restrictions

None.

Example

To display the command history:

```
DGS-3200-10:4# 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-3200-10:4#
```

12-3 dir

Purpose

To display all the commands.

Format

dir

Description

This command is sued to display all the commands.

Parameters

None.

Restrictions

None.

Example

To display all the commands:

```
DGS-3200-10:4# dir
Command: dir


..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear fdb
clear igmp_snooping data_driven_group
clear log
clear mac_based_access_control auth_mac
clear port_security_entry port
clear wac auth_state
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

12-4 config command_history

Purpose

The switch “remembers” the last 40 (maximum) commands you entered. This command lets you configure the number of commands that the switch can recall.

Format

config command_history <value 1-40>

Description

This command is used to configure the number of commands that the switch can recall.

Parameters

Parameters	Description
value	The number of commands (1-40) that the switch can recall.

Restrictions

None.

Example

To configure the number of commands the switch can recall to the last 20 commands:

```
DGS-3200-10:4#config command_history 20
Command: config command_history 20


Success.


DGS-3200-10:4#
```

13 Modify Banner and Prompt Command List

config greeting_message {default}
config command_prompt [<string 16> | username | default]

13-1 config greeting_message

Purpose

To configure the greeting message(or banner).

Format

config greeting_message {default}

Description

This command is used to modify the login banner.

Parameters

Parameters	Description
default	Adding this parameter to the **config greeting_message** command will return the greeting message (banner) to its original factory default entry.

Restrictions

1. 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.
2. The maximum character capacity for the banner is 6*80. (6 Lines and 80 characters per line)
3. 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.
4. Only Administrator-level users can issue this command.

Example

To edit the banner:

```
DGS-3200-10:4#config greeting_message
Command: config greeting_message

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

                         DGS-3200-10 Gigabit Ethernet Switch
                               Command Line Interface

                              Firmware: Build 1.35.B019
             Copyright(C) 2009 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
--------------------------------------------------------------------------------

Success.

DGS-3200-10:4#
```

Response messages

(1). “**Success.**”

When users input a valid greeting message and the setting is accepted by the device.

(2). "**Quit without saving. The current greeting message will not be changed.**”

The user may exit the banner editor by pressing the “Ctrl+c” function key.

(3). "**Fail ! Settings failed.**”

When settings entered are not accepted by the device.

13-2 config command_prompt

Purpose

To configure the command prompt.

Format

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

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-3200-10:4#″). 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.

Parameters

Parameters	Description
string	Enter the new command prompt string of no more than 16 characters.
username	Enter this command to set the login username as the command prompt.
default	Enter this command to return the command prompt to its original factory default value.

Restrictions

1. When users issue the “reset” command, the current command prompt will remain in tact. Yet, issuing the “reset system” will return the command prompt to its original factory default value.
2. Only Administrator-level users can issue this command.

Example

To edit the command prompt:

```
DGS-3200-10:4#config command_prompt DGS-3200-10
Command: config command_prompt DGS-3200-10

Success.

DGS-3200-10:4#
```

Response messages

(1). “**Success.**”

(2). "“**Next possible completions: <string 16> username default.**””

When the prompt string entered exceeds the maximum characters allowed (16).

14 Time and SNTP Command List

```
config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
show sntp
enable sntp
disable sntp
config time <date ddmmmyyyy > <time hh:mm:ss >
config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst [disable
        | repeating {s_week <start_week 1-4,last>
                | s_wday <start_day sun-sat>
                | s_mth <start_mth 1-12>
                | s_time <start_time hh:mm>
                | e_week <end_week 1-4,last>
                | e_wday <end_day sun-sat>
                | e_mth <end_mth 1-12>
                | e_time <end_time hh:mm>
                | offset [30 | 60|90|120]}
        | annual  {s_date <start_date 1-31>
                | s_mth <start_mth 1-12>
                | s_time <start_time hh:mm>
                | e_date <end_date 1-31>
                | e_mth <end_mth 1-12>
                | e_time <end_time hh:mm>
                | offset [30 | 60 | 90 | 120]}]
show time
```

14-1 config sntp

Purpose

To configure SNTP.

Format

```
config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
```

Description

This command is used to change SNTP configurations.

Parameters

Parameters	Description
primary	The SNTP primary server IP address.
secondary	The SNTP secondary server IP address.
poll-interval	The polling interval range is between 30 and 99999 seconds.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure SNTP:

```
DGS-3200-10:4#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-3200-10:4#
```

14-2 show sntp

Purpose

To display SNTP configuration.

Format

show sntp

Description

This command is used to display the current SNTP time source and configuration.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show SNTP:

```
DGS-3200-10:4#show sntp
Command: show sntp

Current Time Scource  : System Clock
SNTP                   : Disabled
SNTP Primary Server   : 10.1.1.1
SNTP Secondary Server : 10.1.1.2
SNTP Poll Interval    : 30 sec

DGS-3200-10:4#
```

14-3 enable sntp

Purpose

To turn on SNTP support.

Format

enable sntp

Description

This command is used to turn on SNTP support.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNTP:

```
DGS-3200-10:4#enable sntp
Command: enable sntp

Success.

DGS-3200-10:4#
```

14-4 disable sntp

Purpose

To turn off SNTP support.

Format

disable sntp

Description

This command is used to turn off SNTP support.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SNTP:

```
DGS-3200-10:4#disable sntp
Command: disable sntp


Success.


DGS-3200-10:4#
```

14-5 config time

Purpose

To configure the time and date settings of the device.

Format

config time <date ddmthyyyy>   <time hh:mm:ss>

Description

This command is used to change the time settings.

Parameters

Parameters	Description
date	system clock date
time	system clock time

Restrictions

Only Administrator-level users can issue this command.

Example

To configure time:

```
DGS-3200-10:4# config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30


Success.


DGS-3200-10:4#
```

14-6 config time_zone

Purpose

To configure the time zone of the device.

Format

config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}

Description

This command is used to change time zone settings.

Parameters

Parameters	Description
operator	operator of time zone + : positive - : negative.
hour	hour of time zone
min	minute of time zone

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the time zone:

```
DGS-3200-10:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30


Success.


DGS-3200-10:4#
```

14-7 config dst

Purpose

To configure Daylight Saving Time of the device.

Format

config dst [disable | repeating {s-week <start_week 1-4,last> | s-day <start_weekday sun-sat> | s-mth <start_mth 1-12> | s-time <start_time hh:mm> | e-week <end_week 1-4,last> | e-day <end_weekday sun-sat> | e-mth <end_mth 1-12> | e-time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s-date <start_date 1-31> | s-mth <start_mth 1-12> | s-time <start_time hh:mm> | e-date <end_date 1-31> | e-mth <end_mth 1-12> | e-time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]

Description

This command is used to change Daylight Saving Time settings.

Parameters

Parameters	Description
disable	Disable the DST of the switch .
repeating	Set the DST to repeating mode .
annual	Set the DST to annual mode.
s_week, e_week	Configure the start/end week number of DST.
s_day, e_day	Configure the start/end day number of DST.
s_mth, e_mth	Configure the start/end month number of DST.
s_time, e_time	Configure the start/end time of DST.
s_date, e_date	Configure the start/end date of DST
offset	Indicates 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.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure time:

```
DGS-3200-10:4#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-3200-10:4#
```

14-8 show time

Purpose

To display time states.

Format

show time

Description

This command is used to display current time states.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show time:

```
DGS-3200-10:4#show time
Command: show time


     Current Time Source   : System Clock
     Boot Time     : 1 Jan 2000  00:00:00
     Current Time : 1 Jan 2000  07:26:28
     Time Zone     : GMT +00:00
     Daylight Saving Time : Disabled
         Offset in Minutes: 60
         Repeating From    : Apr 2nd  Tue 15:00
                   To      : Oct last Sun 00:00
         Annual    From    : 29 Apr 00:00
                   To      : 12 Oct 00:00
DGS-3200-10:4#
```

15 Jumbo Frame Command List

enable jumbo_frame

disable jumbo_frame

show jumbo_frame

15-1 enable jumbo_frame

Purpose

To enable support of Jumbo Frames.

Format

enable jumbo_frame

Description

This command is used to enable support of Jumbo Frames.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable Jumbo Frames:

```
DGS-3200-10:4#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of Jumbo Frame is 10240 Bytes.
Success.

DGS-3200-10:4#
```

15-2 disable jumbo_frame

Purpose

To disable support of Jumbo Frames.

Format

disable jumbo_frame

Description

This command is used to disable support of Jumbo Frames.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable Jumbo Frames:

```
DGS-3200-10:4#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3200-10:4#
```

15-3 show jumbo_frame

Purpose

To display Jumbo Frames.

Format

show jumbo_frame

Description

This command is used to display Jumbo Frames.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display Jumbo Frames:

```
DGS-3200-10:4#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State   : Disabled
Maximum Frame Size : 1536 Bytes

DGS-3200-10:4#
```

16 Single IP Management Command List

enable sim

disable sim

show sim { [candidates { <candidate_id 1-100> } | members { <member_id 1-32> } | group {commander_mac <macaddr>} | neighbor] }

reconfig { member_id <value 1-32> | exit }

config sim_group [add <candidate_id 1-100> { <password> } | delete <member_id 1-32>]

config sim [[commander { group_name <groupname 64> } | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>]

download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}

upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> {[members <mslist> | all]}

16-1 enable sim

Purpose

To enable single IP management.

Format

enable sim

Description

This command is used to configure the single IP management on the switch as enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable single IP management:

```
DGS-3200-10:4#enable sim
Command: enable sim


Success.


DGS-3200-10:4#
```

16-2 disable sim

Purpose

To disable single IP management on the switch.

Format

disable sim

Description

This command is used to configure the single IP management on the switch as disabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable single IP management:

```
DGS-3200-10:4#disable
Command: disable sim


Success.


DGS-3200-10:4#
```

16-3 show sim

Purpose

To display the current information of the specific sorts of devices.

Format

show sim { [candidates { <candidate_id 1-100> } | members { <member_id 1-32> } | group {commander_mac <macaddr>} | neighbor] }

Description

This command is used to display the information of the specific sorts of devices including of self, candidate, member, group, and neighbor.

Parameters

Parameters	Description
candidates	Specifies the candidate devices.
members	Specifies the member devices.
group	Specifies other group devices.

neighbor	Specifies other neighbor devices.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show the self information in detail:

```
DGS-3200-10:4#show sim
Command: show sim


SIM Version          : VER-1.61
Firmware Version     : Build 1.35.B019
Device Name          :
MAC Address          : 00-35-26-11-11-00
Capabilities         : L2
Platform             : DGS-3200-10 L2 Switch
SIM State            : Disabled
Role State           : Candidate
Discovery Interval : 30 sec
Hold Time            : 100 sec


DGS-3200-10:4#
```

To show the candidate information in summary:

```
DGS-3200-10:4#show sim candidate
Command: show sim candidate


ID  MAC Address        Platform /                 Hold  Firmware Device Name
                      Capability                 Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
 1  00-01-02-03-04-00 DGS-3200-10 L2 Switch       40   1.35-B019 aaaaaaaaaaaaaaaa
                                                                  bbbbbbbbbbbbbbb
 2  00-55-55-00-55-00 DES-3326SR L3 Switch      140   4.00-B15 default master


Total Entries: 2


DGS-3200-10:4#
```

To show the member information in summary:

```
DGS-3200-10:4#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-3200-10 L2 Switch      40    1.35-B019 aaaaaaaaaaaaaaaa
                                                               bbbbbbbbbbbbbbb
 2  00-55-55-00-55-00 DES-3326SR L3 Switch      140    4.00-B15 default master

Total Entries: 2

DGS-3200-10:4#
```

To show other groups information in summary:

```
DGS-3200-10:4#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-3200-10 L2 Switch      40    1.35-B019 aaaaaaaaaaaaaaaa
                                                                bbbbbbbbbbbbbbb
 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-3200-10 L2 Switch      40    1.35-B019 aaaaaaaaaaaaaaaa
                                                                bbbbbbbbbbbbbbb
 2  00-55-55-00-55-00

'*' means commander switch.

DGS-3200-10:4#
```

To show an SIM neighbor table:

```
DGS-3200-10:4# show sim neighbor
Command: show sim neighbor

Neighbor Table

Port    MAC Address         Role
------  ------------------  ---------
23      00-35-26-00-11-99   Commander
23      00-35-26-00-11-91   Member
24      00-35-26-00-11-90   Candidate

Total Entries: 3

DGS-3200-10:4#
```

16-4 reconfig

Purpose

To re-Telnet to a member.

Format

reconfig { member_id <value 1-32> | exit }

Description

This command is used to re-Telnet to a member.

Parameters

Parameters	Description
member_id	Specifies the serial number of a member.

Restrictions

Only Administrator-level users can issue this command.

Examples

To re-Telnet to a member:

```
DGS-3200-10:4#reconfig member_id 1
Command: reconfig member_id 1

DGS-3200-10:4#
Login:
```

16-5 config sim_group

Purpose

To configure group information.

Format

config sim_group [add <candidate_id 1-100> { <password> } | delete <member_id 1-32>]

Description

This command is used to configure group information on the switch.

Parameters

Parameters	Description
candidate_id	Add a specific candidate to group.
password	The password of candidate if necessary.
member_id	Remove a specific member from group.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a member:

```
DGS-3200-10:4# config sim_group add 2
Command: config sim_group add 2

Please wait for ACK !!!
SIM Config Success !!!

Success.

DGS-3200-10:4#
```

To delete a member:

```
DGS-3200-10:4# config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!
SIM Config Success !!!

Success.

DGS-3200-10:4#
```

16-6 config sim

Purpose

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>]

Description

This command is used to configure the role state and parameters of discovery protocol on the switch.

Parameters

Parameters	Description
commander	Transfer role to commander.
group_name	If commander, user can update name of group.
candidate	Transfer role to candidate.
dp_interval	The time in seconds between discovery.
hold_time	The time in seconds the device holds the discovery result.

Restrictions

Only Administrator-level users can issue this command.

Examples

To transfer to commander:

```
DGS-3200-10:4# config sim commander
Command: config sim commander


Success.


DGS-3200-10:4#
```

To transfer to candidate:

```
DGS-3200-10:4# config sim candidate
Command: config sim candidate


Success.


DGS-3200-10:4#
```

To update name of group:

```
DGS-3200-10:4#config sim commander group_name mygroup
Command: config sim commander group_name mygroup


Success.


DGS-3200-10:4#
```

To change the time interval of discovery protocol:

```
DGS-3200-10:4# config sim dp_interval 30
Command: config sim dp_interval 30


Success.


DGS-3200-10:4#
```

To change the hold time of discovery protocol:

```
DGS-3200-10:4# config sim hold_time 200
Command: config sim hold_time 200


Success.


DGS-3200-10:4#
```

16-7 download sim_ms

Purpose

To download firmware or configuration to indicated device.

Format

download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}

Description

This command is used to download firmware or configuration from a TFTP server to indicated devices.

Parameters

Parameters	Description
ipaddr	Specifes the ipaddress of TFTP server.
path_filename	Specifes the file path of firmware of configuration in TFTP server.
members	Specifies a range of members which download this firmware or configuration.

Restrictions

Only Administrator-level users can issue this command.

Examples

To download firmware:

```
 DGS-3200-10:4# download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp
members 1
 Commands: download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp
members 1

 This device is updating firmware.  Please wait...

 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-3200-10:4#
```

To download configuration:

```
DGS-3200-10:4# download sim_ms configuratin_from_tftp 10.55.47.1 D:\test.txt 1
Commands: download sim_ms configuratin_from_tftp 10.55.47.1 D:\test.txt 1
<new page>

This device is updating configuration.  Please wait...

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-3200-10:4#
```

16-8 upload sim_ms

Purpose

To upload configuration to TFTP server.

Format

upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> {[members < mslist> | all]}

Description

This command is used to upload configuration from indicated devices to a TFTP server.

Parameters

Parameters	Description
ipaddr	Specifes the IP address of TFTP server.
path_filename	Specifes the file path to store configuration in TFTP server.
members	Specifies the member which upload its configuration.

Restrictions

Only Administrator-level users can issue this command.

Examples

To upload a configuration:

```
 DGS-3200-10:4#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

 Done.

 DGS-3200-10:4#
```

17 Safeguard Engine Command List

```
config safeguard_engine{ state [enable|disable]|
                    utilization{rising <20-100>| falling <20-100>} |
                    trap_log [enable|disable] | mode [ strict | fuzzy] }
show safeguard_engine
```

17-1 config safeguard_engine

Purpose

To configure the safeguard engine.

Format

config safeguard_engine { state [enable|disable]| utilization{rising <20-100>| falling <20-100>} | trap_log [enable|disable] | mode [strict | fuzzy] }

Description

Use this command to configure the safeguard engine for the system.

Parameters

Parameters	Description
state	Configure the safeguard engine state to **enable** or **disable**.
trap_log	Configure the state of safeguard engine related trap/log mechanism to **enable** or **disable**. If set to **enable**, trap and log will be active while the safeguard engine current mode is changed. If set to **disable**, current mode change will not trigger trap and log events.
mode	Determines the controlling method of broadcast traffic. Here are two modes (**strict** and **fuzzy**). In **strict**, the Switch will stop receiving all ‘ARP not to me’ packets (the protocol address of target in ARP packet is the Switch itself). That means no matter what reasons cause the high CPU utilization (may not caused by ARP storm), the Switch reluctantly processes any ’ARP not to me’ packets in exhausted mode. In **fuzzy** mode, the Switch will adjust the bandwidth dynamically depend on some reasonable algorithm .
utilization	Configure the safeguard engine threshold.

	rising	Config utilization rising threshold , the range is between 20%-100% , if the CPU utilization is over the rising threshold, the switch enters exhausted mode.
	falling	Config utilization falling threshold , the range is between 20%-100% , if the CPU utilization is lower than the falling threshold, the switch enters normal mode.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the safeguard engine:

```
DGS-3200-10:4#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-3200-10:4#
```

17-2 show safeguard_engine

Purpose

To show safeguard engine information.

Format

show safeguard_engine

Description

Use this command to display safeguard engine information.

Parameters

None.

Restrictions

None.

Examples

To display safeguard engine information:

```
DGS-3200-10:4#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-3200-10:4#
```

Note: The safeguard engine current status has two modes: exhausted and normal mode.

V. Layer 2

The Layer 2 section includes the following chapters: MSTP, FDB, MAC Notification, Mirror, VLAN/Protocol VLAN, VLAN Trunking, Link Aggregation, LACP Configuration, Traffic Segmentation, Port Security, Static MAC-based VLAN, and Port Egress Filter.

18 MSTP Command List

```
show stp
show stp instance <value 0-15>
show stp ports { <portlist> }
show stp mst_config_id
create stp instance_id <value 1-15>
delete stp instance_id <value 1-15>
config stp instance_id <value 1-15> [add_vlan|remove_vlan] <vidlist>
config stp mst_config_id { name <string> | revision_level <int> }
enable stp
disable stp
config stp version [ mstp | rstp | stp ]
config stp priority <value 0-61440> instance_id <value 0-15>
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 ] | }
config stp ports <portlist> {   external_cost [ auto | <value 1-200000000> ]   |
                             hellotime <value 1-2> |
                             migrate [ yes | no ] |
                             edge [ true | false ] |
                             p2p [ true | false | auto ] |
                             state [ enable | disable ] |
                             fbpdu [ enable | disable ] }
config stp mst_ports <portlist> instance_id <value 0-15>   { internal_cost [ auto | <value
1-200000000> ] | priority <value 0-240> }
```

18-1 show stp

Purpose

To show the bridge parameters global settings. (CIST or MSTI ID=0)

Format

show stp

Description

This command is used to display the bridge parameters global settings.

Parameters

None.

Restrictions

None.

Examples

To display STP:

```
DGS-3200-10:4#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       : 3
Forwarding BPDU     : Enabled

DGS-3200-10:4#
```

18-2 show stp instance

Purpose

To display each instance parameter setting.

Format

show stp instance <value 0-15>

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.

Parameters

Parameters	Description
instance	MSTP instance ID. Instance 0 represents the default instance: CIST. The bridge supports a total 16 Instance（0-15）at most.

Restrictions

None.

Examples

To display STP instances:

```
DGS-3200-10:4#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-3200-10:4#
```

18-3 show stp ports

Purpose

To display port information including parameter settings and operational values.

Format

show stp ports {<portlist>}

Description

This command is used to display each port's parameter settings. If the portlist is not input, all ports will be shown. If there are multi instances on this bridge, the parameters of the port on different instances will be shown.

Parameters

Parameters	Description
ports	Shows parameters of the designated port numbers which are distinguished from the parameters of the bridge.
portlist	One of the CLI Value Types, restricts the input value and format of the ports.

Restrictions

None.

Examples

To show STP ports:

```
DGS-3200-10:4# 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-3200-10:4#
```

18-4 show stp mst_config_id

Purpose

To display the MST Configuration Identification as defined in 802.1's 13.7.

Format

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.

Parameters

Parameters	Description
mst_config_id	If two bridges have the same three elements in **mst_config_id** , that means they are in the same MST region.

Restrictions

None.

Examples

Display the STP MST Config ID:

```
DGS-3200-10:4# 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-3200-10:4#
```

18-5 create stp instance_id

Purpose

To create an MST Instance without mapping the corresponding VLANs yet.

Format

create stp instance_id <value 1-15>

Description

To create a new MST instance independent from the default Instance: CIST（Instance 0). After creating the MST instance, you need to configure the VLANs（using commands in 47-7), or the newly created MST instance will still be in a disabled state .

Parameters

Parameters	Description
instance_id	MSTP instance ID. Instance 0 represents a default instance, CIST. The DUT supports 16 Instance (0-15) at most.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an MSTP instance:

```
DGS-3200-10:4# create stp instance_id 2
Command: create stp instance_id 2

Warning:There is no VLAN mapping to this instance_id!
Success.

DGS-3200-10:4#
```

18-6 delete stp instance_id

Purpose

To delete an MST instance.

Format

delete stp instance_id <value 1-15>

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.

Parameters

Parameters	Description
instance_id	MSTP instance ID. Instance 0 represents the default instance, CIST. The DUT supports 16 instances (0-15) at most.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an MSTP instance:

```
DGS-3200-10:4# delete stp instance_id 2
Command: delete stp instance_id 2


Success.


DGS-3200-10:4#
```

18-7 config stp instance_id

Purpose

To map or remove the VLAN range of the specified MST instance for an existing MST instance.

Format

config stp instance_id <value 1-15> [add_vlan|remove_vlan] <vidlist>

Description

There are two different action types to deal with an MST instance. They are listed as follows:

- **add_vlan**: To map specified VLAN lists to an existing MST instance..
- **remove_vlan**: To delete specified VLAN lists from an existing MST instance.

Parameters

Parameters	Description
instance_id	MSTP instance ID. Instance 0 represents a default instance, CIST. The DUT supports 16 instances (0-15) at most.
add_vlan	Defined action type to configure an MST instance.
remove_vlan	Defined action type to configure an MST instance.
vidlist	Newly added CLI Value Type. It is similar to **<portlist>** type , but the value range is 1 to 4094.

Restrictions

Only Administrator-level users can issue this command.

Examples

To map a VLAN ID to an MSTP instance:

```
DGS-3200-10:4# config stp instance_id 2 add_vlan 1 to 3
Command: config stp instance_id 2 add_vlan 1 to 3


Success.


DGS-3200-10:4#
```

To remove a VLAN ID from an MSTP instance:

```
DGS-3200-10:4# config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2


Success.


DGS-3200-10:4#
```

18-8 config stp mst_config_id

Purpose

To change the name or revision level of the MST configuration identification.

Format

config stp mst_config_id { name <string> | revision_level <int> }

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.

Parameters

Parameters	Description
name	The name given for a specified MST region.
revision_level	The same given name with a different revision level also represents a different MST region.

Restrictions

Only Administrator-level users can issue this command.

Examples

To change the name and revision level of the MST configuration identification:

```
DGS-3200-10:4# config stp mst_config_id name R&D_BlockG revision_level 1

Commands: config stp mst_config_id name R&D_BlockG revision_level 1


Success.


DGS-3200-10:4#
```

18-9 enable stp

Purpose

To enable STP globally.

Format

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. The current chip design dictates that when a user enables the CIST, all MSTIs will be enabled automatically if FORCE_VERSION is set to MSTP(3) and there is at least one VLAN mapped to this instance.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable STP:

```
DGS-3200-10:4# enable stp

Command: enable stp


Success.


DGS-3200-10:4#
```

18-10 disable stp

Purpose

To disable STP globally.

Format

disable stp

Description

To disable STP functionality in every existing instance.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable STP:

```
DGS-3200-10:4# disable stp
Command: disable stp


Success.


DGS-3200-10:4#
```

18-11 config stp version

Purpose

To enable STP globally.

Format

config stp version [mstp | rstp | stp]

Description

This command is used to enable STP gloabally. 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).

Parameters

Parameters	Description
version	To decide to run under which version of STP.

mstp	Multiple Spanning Tree Protocol.
rstp	Rapid Spanning Tree Protocol.
stp	Spanning Tree Protocol.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the STP version:

```
DGS-3200-10:4# config stp version mstp
Command: config stp version mstp


Success.


DGS-3200-10:4#
```

To configure the STP version with the same value of the old configuration:

```
DGS-3200-10:4# config stp version mstp
Command: config stp version mstp


Configure value is the same with current value.
Fail!


DGS-3200-10:4#
```

18-12 config stp priority

Purpose

To configure the instance priority.

Format

config stp priority <value 0-61440> instance_id <value 0-15>

Description

One of the parameters used to select the Root Bridge.

Parameters

Parameters	Description
priority	The bridge priority value must be divisible by 4096.
instance_id	Identifier to distinguish different STP instances.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the STP instance ID:

```
DGS-3200-10:4# config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0


Success.


DGS-3200-10:4#
```

18-13 config stp

Purpose

To configure the bridge management parameters for CIST (instance ID = 0).

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] }

Description

This command is used to configure the bridge parameter global settings.

Parameters

Parameters	Description
maxage	Used to determine if a BPDU is valid. The default value is 20.
maxhops	Used to restrict the forwarded times of one BPDU. The default value is 20.
Hellotime	The default value is 2. This is a per-Bridge parameter in RSTP, it is existed only in STP/RSTP Mode..
forwarddelay	The maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15.
txholdcount	Used 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.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure STP:

```
DGS-3200-10:4# config stp maxage 25
Command: config stp maxage 25


Success.


DGS-3200-10:4#
```

18-14 config stp ports

Purpose

To configure the ports management parameters only at CIST level.

Format

config stp ports <portlist> { external_cost [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] }

Description

This command is used to configure all the parameters of ports, except for Internal Path Cost and Port Priority. The two parameters (Internal Path Cost and Port Priority) are special cases in MSTP and will need another command in 47-13 to use.

Parameters

Parameters	Description
portlist	One of the CLI Value Types, restricts the input value and format of the ports.
external_cost	The path cost between the MST regions from the transmitting Bridge to the CIST Root Bridge. It is only used at CIST level.
hellotime	The default value is 2 . This is a per-Bridge parameter in RSTP, but it becomes a per-Port parameter in MSTP.
migrate	Operation of management in order to specify the port to send MSTP BPDU for a delay time.
edge	Decides 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 BPUD is received.
p2p	Decides if this port is in Full-Duplex or Half-Duplex mode.
state	Decides if this port supports the STP functionality.
restricted_role	Decides if this port is to be selected as Root Port or not. The default value is **false**.
restricted_tcn	Decides if this port is to to propagate a topology change or not. The default value is **false**
fbpdu	Decides if this port will flood STP BPDU when STP functionality is disabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To config STP ports:

```
DGS-3200-10:4# config stp ports 1 external_cost auto
Command: config stp ports 1 external_cost auto


Success.


DGS-3200-10:4#
```

18-15 config stp mst_ports

Purpose

To configure the port management parameters at the CIST (instance ID = 0) or MSTI (instance ID = 1) level.

Format

config stp mst_ports <portlist> instance_id <value 0-15> { internal_cost [auto | <value 1-200000000>] | priority <value 0-240> }

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）.

Parameters

Parameters	Description
mst_ports	Distinguished from the parameters of ports only at the CIST level.
portlist	One of the CLI Value Types, restricts the input value and format of the ports.
instance_id	Instance = 0 represents CIST, Instance from 1 to 15 represents MSTI 1 - MSTI 15 .
internal_cost	The Port Path Cost used in MSTP.
priority	The Port Priority.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure STP MST ports:

```
DGS-3200-10:4# config stp mst_ports 1 instance_id 0 internal_cost auto
Command: config stp mst_ports 1 instance_id 0 internal_cost auto


Success.


DGS-3200-10:4#
```

19 FDB Command List

create fdb <vlan_name 32> <macaddr> port <port>

create multicast_fdb <vlan_name 32> <macaddr>

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

config fdb aging_time <sec 10-875>

config multicast vlan_filtering_mode [vlanid <vidlist>|vlan <vlan_name 32>|all] [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> | mac_address <macaddr> }

show fdb { port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time }

show multicast vlan_filtering_mode {vlanid <vidlist>|vlan <vlan_name 32>}

19-1 create fdb

Purpose

To create a static entry to the unicast MAC address forwarding table (database).

Format

create fdb <vlan_name 32> <macaddr> port <port>

Description

This command is used to make an entry into the switch's unicast MAC address forwarding database.

Parameters

Parameters	Description
vlan_name 32	Specifies a VLAN name associated with a MAC address.
macaddr	The MAC address to be added to the static forwarding table.
port	The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an unicast MAC forwarding:

```
DGS-3200-10:4#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5


Success.

DGS-3200-10:4#
```

19-2 create multicast_fdb

Purpose

To create a static entry to the multicast MAC address forwarding table (database).

Format

create multicast_fdb <vlan_name 32> <macaddr>

Description

This command is used to make an entry into the switch’s multicast MAC address forwarding database.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum length is 32.
macaddr	The multicast MAC address to be added to the static forwarding table.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create multicast MAC forwarding:

```
DGS-3200-10:4# create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00


Success.


DGS-3200-10:4#
```

19-3 config multicast_fdb

Purpose

To configure the switch’s multicast MAC address forwarding database.

Format

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

Description

This command is used to configure the multicast MAC address forwarding table.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum name length is 32.
macaddr	The MAC address that will be added or deleted to the forwarding table.
portlist	Specifies a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add multicast MAC forwarding:

```
DGS-3200-10:4# config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5


Success.

DGS-3200-10:4#
```

19-4 config fdb aging_time

Purpose

To configure the switch's MAC address aging time.

Format

config fdb aging_time <sec 10-875>

Description

This command is used to set the age-out timer for the switch's dynamic unicast MAC address forwarding tables.

Parameters

Parameters	Description
aging_time	Specifies 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 875. The default value is 300.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure MAC address aging time:

```
DGS-3200-10:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3200-10:4#
```

19-5 config multicast vlan_filtering_mode

Purpose

To configure the the multicast packet filtering mode for VLANs.

Format

config multicast vlan_filtering_mode [vlanid <vidlist>|vlan <vlan_name 32> |all] [forward_unregistered_groups|filter_unregistered_groups]

Description

This command is used to configure the multicast packet filtering mode for VLANs.

Parameters

Parameters	Description
vidlist	Specifies VLAN ID list to set.
vlan_name 32|all	Specifies VLAN or all VLANs to set.
forward_unregistered_groups	The filtering mode can be **forward_unregistered_groups**, or **filter_unregistered_groups**.
filter_unregistered_groups	

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the the multicast packet filtering mode for all VLAN:

```
DGS-3200-10:4#config multicast vlan_filtering_mode all forward_unregistered_groups
Command: config multicast port filtering_mode all forward_unregistered_groups


Success.


DGS-3200-10:4#
```

19-6 delete fdb

Purpose

To delete an entry to the switch's forwarding database.

Format

delete fdb <vlan_name 32> <macaddr>

Description

This command is used to delete a permanent FDB entry.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum length is 32.
macaddr	The MAC address to be deleted from the static forwarding table.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a permanent FDB entry:

```
DGS-3200-10:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02


Success.


DGS-3200-10:4#
```

19-7 clear fdb

Purpose

To clear the switch’s forwarding database of all dynamically learned MAC addresses.

Format

clear fdb [vlan <vlan_name 32> | port <port> | all]

Description

This command is used to clear the switch’s forwarding database of all dynamically learned MAC addresses.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum length is 32.
port	The port number corresponding to the dynamically learned MAC address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear all FDB dynamic entries:

```
DGS-3200-10:4#clear fdb all
Command: clear fdb all


Success.


DGS-3200-10:4#
```

19-8 show multicast_fdb

Purpose

To display the contents of the switch’s multicast forwarding database.

Format

show multicast_fdb { vlan <vlan_name 32> | mac_address <macaddr> }

Description

This command is used to display the contents of the switch's multicast forwarding database.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum length is 32.
macaddr	Specifies a MAC address, for which FDB entries will be displayed.
	If no parameter is specified, all multicast fdb entries will be displayed.

Restrictions

None.

Examples

To display multicast MAC address table:

```
DGS-3200-10:4#show multicast_fdb
Command: show multicast_fdb

VLAN Name     : default
MAC Address   : 01-00-5E-00-00-00
Egress Ports  : 1-5,26
Mode          : Static

Total Entries : 1

DGS-3200-10:4#
```

19-9 show fdb

Purpose

To display the current unicast MAC address forwarding database.

Format

show fdb { port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time }

Description

This command is used to display the current unicast MAC address forwarding database.

Parameters

Parameters	Description
port	Displays the entries for one port.
vlan_name 32	Displays the entries for a specific VLAN.
static	Displays all permanent entries.
aging_time	Displays the unicast MAC address aging time.
	If no parameter is specified, the system will display the unicast address table.

Restrictions

None.

Examples

To display unicast MAC address table:

```
DGS-3200-10:4#show fdb
Command: show fdb

Unicast MAC Address Ageing Time = 300

VID   VLAN Name          MAC Address         Port     Type
----  ----------------  -----------------  ------   ----------------
1     default            00-00-00-00-01-02    5      Permanent
1     default            00-01-02-03-04-00   CPU      Self

Total Entries : 2

DGS-3200-10:4#
```

19-10 show multicast vlan_filtering_mode

Purpose

To show the multicast packet filtering mode for VLANs.

Format

show multicast vlan_filtering_mode {vlanid <vidlist>|vlan <vlan_name 32>}

Description

This command is used to display the multicast packet filtering mode for VLANs.

Parameters

Parameters	Description
vidlist	Displays the entries by VLAN ID list.
vlan_name 32	Displays the entries for a specific VLAN.

Restrictions

None.

Examples

To show multicast filtering mode for ports:

```
DGS-3200-10:4#show multicast vlan_filtering_mode
Command: show multicast filtering_mode

VLAN Name                                 Multicast Filter Mode
--------------------------------    -----------------------------
default                               forward_unregistered_groups

DGS-3200-10:4#
```

20 MAC Notification Command List

enable mac_notification

disable mac_notification

config mac_notification{interval <int 1-2147483647>|historysize <int 1-500>}

config mac_notification ports [<portlist>|all] [enable|disable]

show mac_notification

show mac_notification ports{<portlist>}

20-1 enable mac_notification

Purpose

To enable global MAC address table notification on the switch.

Format

enable mac_notification

Description

This command is used to enable global MAC address table notification on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the MAC notification function:

```
DGS-3200-10:4#enable mac_notification
Command: enable mac_notification


Success.


DGS-3200-10:4#
```

20-2 disable mac_notification

Purpose

To disable global MAC address table notification on the switch.

Format

disable mac_notification.

Description

This command is used to disable global MAC address table notification on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the MAC notification function:

```
DGS-3200-10:4#disable mac_notification
Command: disable mac_notification


Success.


DGS-3200-10:4#
```

20-3 config mac_notification

Purpose

To configure the switch's MAC address table notification global settings.

Format

config mac_notification{interval <int 1-2147483647>|historysize <int 1-500>}

Description

This command is used to configure the switch's MAC address table notification global settings.

Parameters

Parameters	Description
interval	The time in seconds between notifications.
historysize	This is the maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the switch's MAC address table notification global settings:

```
DGS-3200-10:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500


Success.


DGS-3200-10:4#
```

20-4 config mac_notification ports

Purpose

To configure the port's MAC address table notification status settings.

Format

config mac_notification ports [<portlist>|all] [enable(3)|disable(2)]

Description

This command is used to configure the port's MAC address table notification status settings.

Parameters

Parameters	Description
portlist	Specifiy a range of ports to be configured.
all	To set all ports in the system, use the "**all**" parameter.
enable	Enable the port's MAC address table notification.
disable	Disable the port's MAC address table notification.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable MAC address table notification for Port 7:

```
DGS-3200-10:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable


Success.


DGS-3200-10:4#
```

20-5 show mac_notification

Purpose

To display the switch's MAC address table notification global settings.

Format

show mac_notification

Description

This command is used to display the switch's MAC address table notification global settings.

Parameters

None.

Restrictions

None.

Examples

To show the switch's MAC address table notification global settings:

```
DGS-3200-10:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State            : Enabled
Interval        : 1
History Size : 500

DGS-3200-10:4#
```

20-6 show mac_notification ports

Purpose

To display the port's MAC address table notification status settings.

Format

show mac_notification ports{<portlist>}

Description

This command is used to display the port's MAC address table notification status settings.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured.

Restrictions

None.

Examples

To display the MAC address table notification status settings of all ports:

```
DGS-3200-10:4#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-3200-10:4#
```

21 Mirror Command List

config mirror port <port> [add|delete] source ports <portlist> [rx | tx | both]
enable mirror
disable mirror
show mirror

21-1 config mirror port

Purpose

To configure a mirror port − a source port pair on the switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe can then be attached to study the traffic crossing the source port in a completely unobtrusive manner.

Format

config mirror port <port> [add |delete] source ports <portlist> [rx|tx|both]

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 or sent by or both is mirrored to the target port.

Parameters

Parameters	Description
port	The port that will receive the packets duplicated at the mirror port.
add	The mirror entry to be added.
delete	The mirror entry to be deleted.
portlist	The port that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port.
rx	Allows the mirroring of only packets received (flowing into) the port or ports in the port list.
tx	Allows the mirroring of only packets sent (flowing out of) the port or ports in the port list.
both	Mirrors all the packets received or sent by the port or ports in the port list.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add mirroring ports:

```
DGS-3200-10:4#config mirror port 6 add source ports 1-5 both
Command: config mirror port 6 add source ports 1-5 both

Success.

DGS-3200-10:4#
```

21-2 enable mirror

Purpose

To enable a previously entered port mirroring configuration.

Format

enable mirror

Description

This command is used to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.

Note: If the target port hasn’t been set, **enable mirror** will not be allowed.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable mirroring configurations:

```
DGS-3200-10:4#enable mirror
Command: enable mirror

Success.

DGS-3200-10:4#
```

21-3 disable mirror

Purpose

To disable a previously entered port mirroring configuration.

Format

disable mirror

Description

This command, combined with the **enable mirror** command above, allows you to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable mirroring configurations:

```
DGS-3200-10:4#disable mirror
Command: disalbe mirror


Success.


DGS-3200-10:4#
```

21-4 show mirror

Purpose

Tto show the current port mirroring configuration on the switch.

Format

show mirror

Description

This command is used to display the current port mirroring configuration on the switch.

Parameters

None.

Restrictions

None.

Examples

To display mirroring configuration:

```
DGS-3200-10:4#show mirror
Command: show mirror

Current Settings
Mirror Status : Disabled
Target Port   : 7
Mirrored Port
            RX:
            TX: 1-5

DGS-3200-10:4#
```

22 VLAN Command List

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

create vlan vlanid <vlanid_list> { advertisement }

delete vlan <vlan_name>

delete vlan vlanid <vlanid_list>

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

config vlan vlanid <vlanid_list> { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]| name <vlan_name>}

config vlan <vlan_name> delete <portlist>

config vlan vlanid <vlanid_list> delete <portlist>

config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] |acceptable_frame[tagged_only | admit_all] pvid<vlanid 1-4094> }

enable gvrp

disable gvrp

show vlan { <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>}

show gvrp {<portlist>}

enable pvid auto_assign

disable pvid auto_assign

show pvid auto_assign

22-1 create vlan

Purpose

To create a VLAN on the switch.

Format

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

create vlan vlanid <vlanid_list> { advertisement }

Description

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

Parameters

Parameters	Description
vlan_name	The name of the VLAN to be created.
vlan vlanid	The VLAN ID of the VLAN to be created.
tag	The VLAN ID of the VLAN to be created. The range is from 2 to 4094.
advertisement	Specifies the VLAN as being able to be advertised out.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4#create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement


Success.


DGS-3200-10:4#
```

22-2 delete vlan

Purpose

To delete a previously configured VLAN on the switch.

Format

delete vlan <vlan_name>

delete vlan vlanid <vlanid_list>

Description

This command is used to delete a previously configured VLAN on the switch.

Parameters

Parameters	Description
vlan_name	The VLAN name of the VLAN to be deleted.
vlan vlanid	The VLAN ID of the VLAN to be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To remove a VLAN v1:

```
DGS-3200-10:4#delete vlan v1
Command: delete vlan v1


Success.


DGS-3200-10:4#
```

22-3 config vlan add ports

Purpose

To add additional ports to a previously configured VLAN.

Format

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

config vlan vlanid <vlanid_list> { [add [tagged | untagged | forbidden] | delete] <portlist> |

Description

This command is used to add ports to the port list of a previously configured VLAN. You can specifiy the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN you want to add ports to.
vlan vlanid	The VLAN ID of the VLAN you want to add ports to.
tagged	Specifies the additional ports as tagged.
untagged	Specifies the additional ports as untagged.
forbidden	Specifies the additional ports as forbidden.
portlist	A range of ports to add to the VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add 4 through 8 as tagged ports to the VLAN v1:

```
DGS-3200-10:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8


Success.


DGS-3200-10:4#
```

22-4 config vlan delete ports

Purpose

To delete one or more ports from a previously configured VLAN.

Format

config vlan <vlan_name 32> delete <portlist>

config vlan vlanid <vlanid_list> delete <portlist>

Description

This command is used to delete one or more ports from a previously configured VLAN.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN you want to delete ports from.
vlan vlanid	The VLAN ID of the VLAN you want to delete ports from.
portlist	Specifies a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete ports 4 through 8 from VLAN v1:

```
DGS-3200-10:4#config vlan v1 delete 4-8
Command: config vlan v1 delete 4-8


Success.


DGS-3200-10:4#
```

22-5 config vlan advertisement

Purpose

To enable or disable the VLAN advertisement.

Format

config vlan vlanid <vidlist> advertisement [enable | disable]

Description

This command is used to enable or disable the VLAN advertisement.

Parameters

Parameters	Description
vlan vlanid	The VLAN ID of the VLAN on which you want to configure.
advertisement	Join GVRP or not. If not, the VLAN can't join dynamically

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the VLAN default advertisement:

```
DGS-3200-10:4#config vlan default advertisement enable
Command: config vlan default advertisement enable


Success.


DGS-3200-10:4#
```

22-6 config gvrp

Purpose

To set the ingress checking status and the sending and receiving of GVRP information.

Format

config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] pvid<vlanid 1-4094> }

Description

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

Parameter

Parameters	Description	
portlist	A range of ports for which you want ingress checking. The beginning and end of the port list range are separated by a dash.	
state	Enables or disables GVRP for the ports specified in the port list.	
ingress_checking	Enables or disables ingress checking for the specified portlist.	
acceptable_frame	The type of frame will be accepted by the port.	
	tagged_only	Only tagged frame will be received.
	admit_all	Both tagged and untagged will be accepted.
pvid	Specified the default VLAN will associated with the port.	

Restrictions

Only Administrator-level users can issue this command.

Example

To set the ingress checking status and send and receive GVRP information:

```
 DGS-3200-10:4#config gvrp_5 state enable ingress_checking enable acceptable_
 frame tagged_only pvid 2
 Command: config gvrp_5 state enable ingress_checking enable acceptable_frame
tagged_only pvid 2

 Success

 DGS-3200-10:4#
```

22-7 enable gvrp

Purpose

To enable the Generic VLAN Registration Protocol (GVRP).

Format

enable gvrp

Description

This command is used to enable the Generic VLAN Registration Protocol (GVRP). The default setting is disabled.

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3200-10:4#enable gvrp
Command: enable gvrp


Success.


DGS-3200-10:4#
```

22-8 disable gvrp

Purpose

To disable Generic VLAN Registration Protocol (GVRP).

Format

disable gvrp

Description

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

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable Generic VLAN Registration Protocol (GVRP) :

```
DGS-3200-10:4#disable gvrp
Command: disable gvrp


Success.


DGS-3200-10:4#
```

22-9 show vlan

Purpose

To display the VLAN information including of parameters setting and operational value.

Format

show vlan { <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>}

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.

Parameters

Parameters	Description
vlan_name	The name of the VLAN to be displayed.
vlanid	The VLAN ID number to be displayed.
ports	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.

Examples

To display VLAN settings:

```
DGS-3200-10:4#show vlan
Command: show vlan

VID             : 1           VLAN Name        : default
VLAN TYPE       : static     Advertisement    : Enabled
Member ports    : 1-7
Static ports    : 1-6
Current Tagged ports:
Current Untagged ports  : 1-7
Static Tagged ports:
Static Untagged ports   : 1-6
Forbidden ports :

Total Entries : 1

DGS-3200-10:4#
```

To display VLAN port settings:

```
DGS-3200-10:4#show vlan ports 1-2
Command: show vlan ports 1-2

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

DGS-3200-10:4#
```

22-10 show gvrp

Purpose

To display the GVRP status for a port list on the switch.

Format

show gvrp {<portlist>}

Description

This command is used to display the GVRP status for a port list on the switch.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be displayed.
	If no parameter is specified, the system will display GVRP information for all ports.

Restrictions

None.

Example

To display the 802.1q port setting for ports 1 through 6:

```
DGS-3200-10:4#show gvrp 1-6
Command: show gvrp 1-6

Global GVRP : Enabled

Port    PVID  GVRP      Ingress Checking  Acceptable Frame Type
------  ----  --------  ----------------  ---------------------------
1       2     Enabled   Enabled            Only VLAN-tagged frames
2       2     Enabled   Enabled            Only VLAN-tagged frames
3       2     Enabled   Enabled            Only VLAN-tagged frames
4       2     Enabled   Enabled            Only VLAN-tagged frames
5       2     Enabled   Enabled            Only VLAN-tagged frames
6       1     Disabled  Enabled            All Frames

Total Entries : 6

DGS-3200-10:4#
```

22-11 enable pvid auto_assign

Purpose

To enable auto assignment of PVID.

Format

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”. The default setting is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the auto-assign PVID:

```
DGS-3200-10::4#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3200-10::4#
```

22-12 disable pvid auto_assign

Purpose

To disable auto assignment of PVID.

Format

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”. The default setting is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the auto-assign PVID:

```
DGS-3200-10::4#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3200-10::4#
```

22-13 show pvid auto_assign

Purpose

To display the PVID auto-assigment state.

Format

show pvid auto_assign

Description

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

Parameters

None.

Restrictions

You must have user-level privileges.

Example

To display the PVID auto-assignment state:

```
DGS-3200-10::4#show pvid auto_assign


PVID Auto-assignment: Enabled.


DGS-3200-10::4#
```

23 Protocol VLAN Command List

create dot1v_protocol_group group_id <id 1-8> {group_name <name 1-32>}
config dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32>] add protocol [ethernet_2| ieee802.3_snap| ieee802.3_llc] <protocol_value>
config dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32>] delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] < protocol_value>
delete dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32>| all]
show dot1v_protocol_group {group_id <id 1-8> | group_name <name 1-32>}
config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id 1-8> | group_name <name 1-32>] [vlan< vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>} | delete protocol_group [group_id <id 1-8>|all]]
show port dot1v {ports <portlist>}

23-1 create dot1v_protocol_group

Purpose

To create a protocol group for the protocol VLAN function.

Format

create dot1v_protocol_group group_id <id 1-8> {group_name <name 1-32>}

Description

This command is used to create a protocol group for the protocol VLAN function.

Parameters

Parameters	Description
group_id	The ID of the protocol group which is used to identify a set of protocols.
group_name	The name of the protocol group. The maximum length is 32 characters. If a group name is not specified, the group name will be automatically generated in accordance with ProtocolGroup+group_id. For example, the auto-generated name for group ID 2 is ProtocolGroup2. If the auto-generated name is in conflict with an existing group, an alternative name will be used in accordance with ProtocolGroup+group_id+ALT+num. The value for num starts with 1. If it is still in conflict, then subsequent number will be used instead. For example, the auto-generated name for group ID 1 is

	"ProtocolGroup1." If this name already exists, then "ProtocolGroup1ALT1" will be used instead.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a protocol group:

```
DGS-3200-10:4#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-3200-10:4#
```

23-2 config dot1v_protocol_group add protocol

Purpose

To add a protocol to a protocol group.

Format

config dot1v_protocol_group [group_id <id 1-8>| group_name <name 1-32>] add protocol [ethernet_2| ieee802.3_snap|ieee802.3_llc] < protocol_value>

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.

Parameters

Parameters	Description
group_id	The ID of the protocol group which is used to identify a set of protocols.
group_name	The name of the protocol group.
protocol_value	The protocol value is used to identify a protocol of the frame type specified. 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-level users can issue this command.

Example

To add a protocol IPv6 to protocol group 4:

```
DGS-3200-10:4# 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-3200-10:4#
```

23-3 config dot1v_protocol_group delete protocol

Purpose

To delete a protocol from a protocol group.

Format

config dot1v_protocol_group [group_id <id 1-8>| group_name <name 1-32>] delete protocol [ethernet_2| ieee802.3_snap| ieee802.3_llc] < protocol_value>

Description

This command is used to delete a protocol from a protocol group.

Parameters

Parameters	Description
group_id	Specifies the group ID to be deleted.
group_name	The name of the protocol group.
protocol_value	The protocol value is used to identify a protocol of the frame type specified. 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-level users can issue this command.

Example

To delete a protocol IPv6 from protocol group ID 4:

```
DGS-3200-10:4# 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-3200-10:4#
```

23-4 delete dot1v_protocol_group

Purpose

To delete a protocol group.

Format

delete dot1v_protocol_group [group_id <id 1-8>| group_name <name 1-32>| all]

Description

This command is used to delete a protocol group.

Parameters

Parameters	Description
group_id	Specifies the group ID to be deleted.
group_name	The name of the protocol group.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete protocol group ID 4:

```
DGS-3200-10:4# delete dot1v_protocol_group group_id 4
Command: delete dot1v_protocol_group group_id 4


Success.
DGS-3200-10:4#
```

23-5 show dot1v_protocol_group

Purpose

To display the protocols defined in a protocol group.

Format

show dot1v_protocol_group {group_id <id 1-8> | group_name <name 1-32->}

Description

This command is used to display the protocols defined in protocol groups.

Parameters

Parameters	Description
group_id	Specifies the ID of the group to be displayed if group id is not specified, all configured protocol groups will be displayed
group_name	The name of the protocol group.

Restrictions

None.

Example

To display protocol group ID 4:

```
DGS-3200-10:4# 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

Success.
DGS-3200-10:4#
```

23-6 config port dot1v

Purpose

To assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured.

Format

config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id 1-8>| group_name <name 1-32>] [vlan < vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>} | delete protocol_group [group_id <id 1-32>|all]]

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.

Parameters

Parameters	Description
portlist	Specifies a range of ports to apply this command.
group_id	Group ID of the protocol group.
group_name	The name of the protocol group.
vlan	VLAN that is to be associated with this protocol group on this port.
vlan_id	Specifies the VLAN ID .
priority	Specifies the priority to be associated with the packet which has been classified to the specified VLAN by the protocol.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the group ID 4 on port 3 to be associated with VLAN 2:

```
DGS-3200-10:4# 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-3200-10:4#
```

23-7 show port dot1v

Purpose

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>}

Description

This command is used to display the VLAN to be associated with untagged packets ingressed from a port based on the protocol group.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be displayed. If not specified, information for all ports will be displayed.

Restrictions

None.

Example

To display the protocol VLAN information for ports 1 to 2:

```
DGS-3200-10:4# show port dot1v ports 1-2
Command: show port dot1v ports 1-2



Port : 1
Protocol Group ID      VLAN Name
----------------- --------------------------------
1                      default
2                      vlan_2
3                      vlan_3
4                      vlan_4

Port : 2 ,
Protocol Group ID      VLAN Name
----------------- --------------------------------
1                      vlan_2
2                      vlan_3
3                      vlan_4
4                      vlan_5

Success.
DGS-3200-10:4#
```

24 VLAN Trunking Command List

enable vlan_trunk

disable vlan_trunk

config vlan_trunk ports [<portlist>|all] state [enable|disable]

show vlan_trunk

24-1 enable vlan_trunk

Purpose

To enable the VLAN trunking function.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable VLAN trunking:

```
DGS-3200-10:4#enable vlan_trunk
Command: enable vlan_trunk


Success


DGS-3200-10:4#
```

24-2 disable vlan_trunk

Purpose

To disable the VLAN trunking function.

Format

disable vlan_trunk

Description

This command is used to disable VLAN trunking.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable VLAN trunking:

```
DGS-3200-10:4#disable vlan_trunk
Command: disable vlan_trunk


Success.


DGS-3200-10:4#
```

24-3 config vlan_trunk

Purpose

To configure a port as a VLAN trunking port.

Format

config vlan_trunk ports [<portlist>|all] | state [enabled|disabled]

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. However, this setting will disappear as the aggregated link is broken, and the VLAN trunking setting of the individual port will follow the original setting of the port. If the command is applied to link aggregation member port excluding the master, the command will be rejected. 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.

Parameters

Parameters	Description
portlist	Specify the list of ports to be configured.
enable	Specifies that the port is a VLAN trunking port.
disable	Specifies that the port is not a VLAN trunking port.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure ports 1 to 5 as VLAN trunking ports:

```
DGS-3200-10:4#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DGS-3200-10:4#
```

To configure port 6 as an LA-1 member port and port 7 as an LA-2 master port:

```
DGS-3200-10:4# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

The link aggregation member port cannot be configured.
Fail.

DGS-3200-10:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3200-10:4# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

The link aggregation member port cannot be configured.
Fail.

DGS-3200-10:4#
```

To configure port 6 as an LA-1 member port and port 7 as an LA-1 master port:

```
DGS-3200-10:4# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DGS-3200-10:4#
```

Ports 6 and 7 have different VLAN configurations before enabling VLAN trunking. To configure port 6 as an LA-1 member port and port 7 as an LA-1 master port :

```
DGS-3200-10:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

The link aggregation needs to be deleted first.
Fail.
```

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-3200-10:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3200-10:4# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DGS-3200-10:4#
```

24-4 show vlan_trunk

Purpose

To show the VLAN trunking configuration.

Format

show vlan_trunk

Description

This command is used to display VLAN trunking information.

Parameters

None.

Restrictions

None.

Example

To display the current VLAN trunking information:

```
DGS-3200-10:4#show vlan_trunk
Command: show vlan_trunk


VLAN Trunk             :Enable
VLAN Trunk Port        :1-5,7


DGS-3200-10:4#
```

25 Link Aggregation Command List

create link_aggregation group_id <value 1-5> {type [lacp | static] }

delete link_aggregation group_id <value 1-5>

config link_aggregation group_id <value 1-5> {master_port <port> | ports <portlist> | state [enable|disable]}

config link_aggregation algorithm [mac_source_dest | ip_source_dest]

show link_aggregation {group_id <value 1-5> | algorithm}

25-1 create link_aggregation group_id

Purpose

To create a link aggregation group on the switch.

Format

create link_aggregation group_id <value 1-5> {type [lacp | static] }

Description

This command is used to create a link aggregation group.

Parameters

Parameters	Description
group_id	Specifies the group ID. The group number identifies each of the groups. The switch allows up to five link aggregation groups to be configured.
type	Specifies the group type is belong to static or LACP. If type is not specified, the default is the static type.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a link aggregation group:

```
DGS-3200-10:4#create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp


Success


DGS-3200-10:4#
```

25-2 delete link_aggregation group_id

Purpose

To delete a previously configured link aggregation group.

Format

delete link_aggregation group_id <value 1-5>

Description

This command is used to delete a previously configured link aggregation group.

Parameters

Parameters	Description
group_id	The specifies the group ID. The group number identifies each of the groups. The switch allows up to five link aggregation groups to be configured.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a link aggregation group:

```
DGS-3200-10:4#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3


Success.


DGS-3200-10:4#
```

25-3 config link_aggregation

Purpose

To configure a previously created link aggregation group.

Format

config link_aggregation group_id <value> {master_port <port> | ports <portlist> | state [enabled|disabled]}

Description

This command allows you to configure a link aggregation group that was created with the **create link_aggregation** command above.

Parameters

Parameters	Description
group_id	Specifies the group ID. The group number identifies each of the groups. The switch allows up to five link aggregation groups to be configured.
master_port	The master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.
ports	Specifies a range of ports that will belong to the link aggregation group.
state	Allows you to enable or disable the specified link aggregation group. If configuring an LACP group, the ports' state machine will start.

Restrictions

Only Administrator-level users can issue this command.

Example

To define a load-sharing group of ports, group-id 1, master port 7:

```
DGS-3200-10:4#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-3200-10:4#
```

25-4 config link_aggregation algorithm

Purpose

To configure the link aggregation algorithm.

Format

config link_aggregation algorithm [mac_source_dest | ip_source_dest]

Description

This command is used to configure the part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data. This feature is only available when using the address-based load-sharing algorithm.

Parameters

Parameters	Description
mac_source_dest	Indicates that the switch should examine the MAC source and destination address.
ip_source_dest	Indicates that the switch should examine the IP source and destination address.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the link aggregation algorithm for mac-source-dest:

```
DGS-3200-10:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest


Success.


DGS-3200-10:4#
```

25-5 show link_aggregation

Purpose

To display the current link aggregation configuration on the switch.

Format

show link_aggregation {group_id <value> | algorithm}

Description

This command is used to display the current link aggregation configuration of the switch.

Parameters

Parameters	Description
group_id	Specifies the group ID. The group number identifies each of the groups. The switch allows up to five link aggregation groups to be configured.
algorithm	Allows you to specify the display of link aggregation by the algorithm in use by that group.
	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-3200-10:4#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

DGS-3200-10:4#
```

To display the current link aggregation configuration when link aggregation is disabled:

```
DGS-3200-10:4#show link
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

DGS-3200-10:4#
```

26 LACP Configuration Command List

config lacp_ports <portlist> mode [active|passive]

show lacp_ports {<portlist>}

26-1 config lacp_ports

Purpose

To configure the current mode of LACP of port .

Format

config lacp_ports <portlist> mode [active|passive]

Description

This command is used to configure per-port LACP mode.

Parameters

Parameters	Description
portlist	Specified a range of ports to be configured.
mode	**active/passive**

Restrictions

Only Administrator-level users can issue this command.

Example

To configure port LACP mode for ports 1 to 10:

```
DGS-3200-10:4#config lacp_port 1-10 mode active
Command: config lacp_port 1-10 mode active


Success.


DGS-3200-10:4#
```

26-2 show lacp_ports

Purpose

To display the current mode of LACP of port(s).

Format

show lacp_ports <portlist>

Description

This command is used to display per-port LACP mode.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured.
	If no parameter is specified, the system will display current LACP and all port status.

Restrictions

None.

Example

To display the current port LACP mode for all ports on the switch:

```
DGS-3200-10:4#show lacp_ports
Command: show lacp_ports

Port    Activity
------  --------
1       Active
2       Active
3       Active
4       Active
5       Active
6       Active
7       Active
8       Active
9       Active
10      Active

DGS-3200-10:4#
```

27 Traffic Segmentation Command List

config traffic_segmentation [<portlist>|all] forward_list[null|all|<portlist>]

show traffic_segmentation {<portlist>}

27-1 config traffic_segmentation

Purpose

To configure traffic segmentation.

Format

config traffic_segmentation [<portlist>|all] forward_list [null | all | <portlist>]

Description

This command is used to configure traffic segmentation.

Parameters

Parameters	Description	
portlist	Specifes a range of ports to be configured.	
forward_list	Specifies a range of port forwarding domains.	
	portlist	Specifes a range of ports to be configured.
	null	Specifies a range of port forwarding domain is null.

Restrictions

Only Administrator-level users can issue this command. The forwarding domain is restricted to Bridge Traffic only.

Example

To configure traffic segmentation:

```
DGS-3200-10:4# config traffic_segmentation 1-6 forward_list 7-8
Command: config traffic_segmentation 1-6 forward_list 7-8


Success.


DGS-3200-10:4#
```

27-2 show traffic_segmentation

Purpose

To display the current traffic segmentation table.

Format

show traffic_segmentation {<portlist>}

Description

This command is used to display the traffic segmentation table.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be displayed.
	If no parameter is specified, the system will display all current traffic segmentation tables.

Restrictions

None.

Example

To display the traffic segmentation table:

```
DGS-3200-10:4# show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port    Forward Portlist
------  --------------------------------------------------
1       1-10
2       1-10
3       1-10
4       1-10
5       1-10
6       1-10
7       1-10
8       1-10

DGS-3200-10:4#
```

28 Port Security Command List

config port_security ports | all] { admin_state [enable | disable] |max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent|DeleteOnTimeout|DeleteOnReset]
delete port_security_entry vlan_name<vlan_name 32> port <port> mac_address <macaddr>
clear port_security_entry port <portlist>
show port_security {ports <portlist>}
enable port_security trap_log
disable port_security trap_log

28-1 config port_security

Purpose

To configure port security.

Format

config port_security ports| all] { admin_state [enable | disable] |max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent|DeleteOnTimeout|DeleteOnReset])

Description

This command is used to configure port security. It includes admin state, maximum learning address, and lock address mode.

Parameters

<table>
<tr><th>Parameters</th><th colspan="2">Description</th></tr>
<tr><td><b>portlist</b></td><td colspan="2">Specifies a range of ports to be configured.(port number).</td></tr>
<tr><td><b>all</b></td><td colspan="2">All ports be configured.</td></tr>
<tr><td><b>admin_state</b></td><td colspan="2">Allows the port security to be enabled or disabled for the ports specified in the port list.</td></tr>
<tr><td><b>max_learning_addr</b></td><td colspan="2">The maximum number of address learning set to the ports specified in the portlist. The maximum number of entries is 64.</td></tr>
<tr><td rowspan="3"><b>lock_address_mode</b></td><td colspan="2">Indicates locking address mode.</td></tr>
<tr><td><b>Permanent</b></td><td>The locked addresses will not be aged out after aging timer expire.</td></tr>
<tr><td><b>DeleteOnTimeout</b></td><td>The locked addresses can be aged out after aging timer expire</td></tr>
</table>

	DeleteOnReset	never age out the locked addresses unless restart the system to prevent from port movement or intrusion.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the port security setting for port 6:

```
DGS-3200-10:4#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 16
lock_address_mode Permanent

Success.

DGS-3200-10:4#
```

28-2 delete port_security_entry

Purpose

To delete a port security entry by MAC address, port number, and VLAN ID.

Format

delete port_security_entry vlan_name <vlan_name 32> port <port> mac_address <macaddr>

Description

This command is used to delete a port security entry by mac address, port number, and VLAN ID.

Parameters

Parameters	Description
vlan_name 32	The VLAN name the port belongs to.
mac_address	The MAC address to be deleted which was learned by the port.
portlist	The port number which has learned the MAC .

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a default route from the routing table for port 6:

```
DGS-3200-10:4#delete port_security_entry vlan_name default mac_address
00-01-30-10-2C-C7 port 6
Command: delete port_security_entry vlan_name default mac_address
00-01-30-10-2C-C7 port 6

Success.

DGS-3200-10:4#
```

28-3 clear port_security_entry

Purpose

To clear the MAC entries learned from the specified port(s) for the port security function.

Format

clear port_security_entry port <portlist>.

Description

This command is used to clear the MAC entries learned from the specified port(s) for the port security function.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured.(UnitID:port number).

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear port security entry for port 6:

```
DGS-3200-10:4#clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DGS-3200-10:4#
```

28-4 show port_security

Purpose

To display the port security related information of the switch ports.

Format

show port_security {ports <portlist>}

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.

Parameters

None.

Restrictions

None.

Examples

To display the port security information of switch ports 1 to 6:

```
DGS-3200-10:4# show port_security ports 1-6
Command: show port_security ports 1-6

Port_security Trap/Log : Enabled

Port    Admin State  Max. Learning Addr.  Lock Address Mode
------  -----------  -------------------  -----------------
1      Disabled     1                    DeleteOnReset
2      Disabled     1                    DeleteOnReset
3      Disabled     1                    DeleteOnReset
4      Disabled     1                    DeleteOnReset
5      Disabled     1                    DeleteOnReset
6      Enabled      10                   Permanent

DGS-3200-10:4#
```

28-5 enable port_security trap_log

Purpose

To enable the port security trap/log.

Format

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 informationt and the relevant information will be logged.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable a port security trap:

```
DGS-3200-10:4# enable port_security trap_log
Command: enable port_security trap_log


Success.


DGS-3200-10:4#
```

28-6 disable port_security trap_log

Purpose

To disable a port security trap/log.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To prevent a port security trap from being sent from the switch:

```
DGS-3200-10:4# disable port_security trap_log
Command: disable port_security trap_log


Success.


DGS-3200-10:4#
```

29 Static MAC-based VLAN Command List

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>] }

show mac_based_vlan {mac_address <macaddr> | vlan <vlan_name 32>|<vlanid <vlanid 1-4094>}

29-1 create mac_based_vlan

Purpose

To create a static MAC-based VLAN entry.

Format

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Description

This command is used to create static MAC-based VLAN entries. When an entry is created for a port, the port will automatically become the untagged member port of the specificed VLAN. When a static MAC-based VLAN entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN regardless of the authentication function operating on this port.

Parameters

Parameters	Description
mac_address	The MAC address.
vlan	The VLAN to be associated with the MAC address.
vlanid	The VLAN ID to be associated with the MAC address.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a static MAC-based VLAN entry:

```
DGS-3200-10:4# 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-3200-10:4#
```

29-2 delete mac_based_vlan

Purpose

To delete a static MAC-based VLAN entry.

Format

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>] }

Description

This command is used to delete a database entry. If the MAC address and VLAN are not specified, all static entries associated with the port will be removed.

Parameters

Parameters	Description
mac_address	The MAC address.
vlan	The VLAN to be associated with the MAC address.
vlanid	The VLAN ID to be associated with the MAC address.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a static MAC-based VLAN entry:

```
DGS-3200-10:4# 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-3200-10:4#
```

29-3 show mac_based_vlan

Purpose

To display a static MAC-based VLAN entry.

Format

show mac_based_vlan {mac_address <macaddr> | vlan <vlan_name 32>|<vlanid <vlanid 1-4094>}

Description

This command is used to display the static MAC-based VLAN entry.

Parameters

Parameters	Description
mac_address vlan	Specifies the entry that you would like to display.
vlanid	The VLAN ID to be associated with the MAC address.

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 entry:

```
DGS-3200-10:4# show mac_based_vlan


    MAC Address          VLAN          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 AC
00-a2-44-17-32-98      400            Active        WAC

Total Entries : 4


DGS-3200-10:4#
```

30 Port Egress Filter Command List

config egress_filter ports [<portlist> | all] { unicast [enable|disable] | multicast [enable| disable] }

show egress_filter ports {<portlist>}

30-1 config egress_filter ports

Purpose

To configure the state of egress filtering on a specific port.

Format

config egress_filter ports [<portlist> | all] { unicast [enable|disable] | multicast [enable| disable] }

Description

This command is used to configure the state of egress filters on specified ports.

Parameters

Parameters	Description
portlist	Specifies the portlist.
unicast	Specifies the egress filter state of destination lookup fail packets. **disable**: Unknown unicast packets are not filtered and may be forwarded to this port. **enable**: Unknown unicast packets are filtered and are not forwarded to this port.
multicast	Specifies the egress filter state of unregistered multicast packets. **disable**: Unregistered multicast packets are not filtered and may be forwarded to this port. **enable**: Unregistered multicast packets are filtered and are not forwarded to this port.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure an egress filter:

```
DGS-3200-10:4# config egress_filter 6 unicast enable multicast enable
Command: config egress_filter 6 unicast enable multicast enable


Success.


DGS-3200-10:4#
```

30-2 show egress_filter ports

Purpose

To display the port egress filter configuration.

Format

show egress_filter ports {<portlist>}

Description

This command is used to show port egress filter configuration.

Parameters

Parameters	Description
portlist	Specifies the port list.

Restrictions

None.

Examples

To display the egress filter for port 6:

```
DGS-3200-10:4# show  egress_filter ports 6
Command: show egress_filter ports 6


Port    Unicast    Multicast
----    -------    -----------
6       Enabled    Enabled


DGS-3200-10:4#
```

VI. IP

The IP section includes the following chapters: Basic IP, Auto Config, Routing Table, ARP, and Loopback Detection.

31 Basic IP Command List

config ipif <ipif_name 12>[{ipaddress<network_address> |vlan<vlan_name 32>|state [enable|disable]}| bootp |dhcp | ipv6 ipv6address <ipv6networkaddr>]

create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {state [enable|disable]}

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

enable ipif [<ipif_name 12> | all]

disable ipif [<ipif_name 12> | all]

show ipif {<ipif_name 12>}

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

show ipif_ipv6_link_local_auto {<ipif_name 12>}

31-1 config ipif

Purpose

To configure the specified IP interface.

Format

config ipif <ipif_name 12>[{ipaddress<network_address> |vlan<vlan_name 32>| state [enable|disable]}| bootp |dhcp | ipv6 ipv6address <ipv6networkaddr>]

Description

This command is used to configure the specified IP interface.

Parameters

Parameters	Description
ipif_name	The name of the IP interface.
vlan_name	The name of the VLAN corresponding to the IP interface.
network_address	The IP address and netmask of th IP interface to be created. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).
state	Allows you to enable or disable the IP interface.
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.
ipv6networkaddr	The IPv6 address and subnet prefix of the IPV6 address to be create.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the System IP interface:

```
DGS-3200-10:4# config ipif System vlan v1
Command: config ipif System vlan v1


Success.


DGS-3200-10:4#
```

31-2 create ipif

Purpose

To create an IPv6 interface for IPv6 addresses.

Format

create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {state [enable|disable]}

Description

This command is used to create an IP interface for IPv6 only. This interface can only be configured with an IPv6 address. Because only one IPV6 interface is supported, when the System interface already has some IPV6 addresses, executing this command will fail.
Note: The Switch only supports one IP interface for IPV6 addresses.

Parameters

Parameters	Description
ipif_name	The name of the interface.
network_address	This parameter is not supported in the current release.
vlan_name	The name of the VLAN corresponding to the IP interface.
state	The state of the IP interface.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an IP interface “petrovic1”:

```
DGS-3200-10:4# create ipif ip petrovic1
Command: create ipif ipif ip petrovic1


Success.


DGS-3200-10:4#
```

31-3 delete ipif

Purpose

To delete an interface or an IPv6 address.

Format

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

Description

This command is used to delete an IPv6 interface or an IPv6 address.

Parameters

Parameters	Description
ipif_name	The name of the interface.
ipv6networkaddr	The IPv6 network address which want to be deleted by administrator.
all	All IP interface except the System IP interface will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete interface “petrovic1.”

```
DGS-3200-10:4#delete ipif petrovic1
Command: delete ipif petrovic1


Success.


DGS-3200-10:4#
```

31-4 enable ipif

Purpose

To enable the administrative state for an interface.

Format

enable ipif [<ipif_name 12> | all]

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.

Parameters

Parameters	Description
ipif_name	The name of the interface.
all	All of the IP interfaces.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the state for interface “petrovic1”:

```
DGS-3200-10:4#enable ipif petrovic1
Command: enable ipif petrovic1


Success.


DGS-3200-10:4#
```

31-5 disable ipif

Purpose

To disable the administrative state for an interface.

Format

disable ipif [<ipif_name 12> | all]

Description

This command is used to disable the state of an interface.

Parameters

Parameters	Description
ipif_name	The name of the interface.
all	All the IP interface

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the state for an interface:

```
DGS-3200-10:4#disable ipif petrovic1
Command: disable ipif petrovic1


Success.


DGS-3200-10:4#
```

31-6 show ipif

Purpose

To display IP interface settings.

Format

show ipif {<ipif_name 12>}

Description

This command is used to display IP interface settings.

Parameters

Parameters	Description
ipif_name	The name of the interface.

Restrictions

None.

Examples

To display IP interface settings:

```
DGS-3200-10:4# show ipif
Command: show ipif

IP Interface Settings

IP Interface               : System
IP Address                 : 10.90.90.90     (MANUAL)
Subnet Mask                : 255.0.0.0
VLAN Name                  : v1
Interface Admin. State     : Enabled
Link Status                : Link UP
Member Ports               : 1-10

Total Entries : 1

DGS-3200-10:4#
```

31-7 enable ipif_ipv6_link_local_auto

Purpose

To enable the auto configuration of link local address when no IPv6 address is configured.

Format

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

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.

Parameters

Parameters	Description
ipif_name	The name of the interface.
all	All the IP interfaces.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the automatic configuration of link local address for an interface:

```
DGS-3200-10:4#enable ipif_ipv6_link_local_auto interface1
Command: enable ipif_ipv6_link_local_auto interface1

Success.

DGS-3200-10:4#
```

31-8 disable ipif_ipv6_link_local_auto

Purpose

To disable the auto configuration of link local address when no IPv6 address is configured.

Format

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Description

This command is used to disable the auto configuration of link local address when no IPv6 address is explicitly configured.

Parameters

Parameters	Description
ipif_name	The name of the interface.
all	All the IP interface

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the automatic configuration of link local address for an interface.

```
DGS-3200-10:4#disable ipif_ipv6_link_local_auto interface1
Command: disable ipif_ipv6_link_local_auto interface1

Success.

DGS-3200-10:4#
```

31-9 show ipif_ipv6_link_local_auto

Purpose

To display the link local address automatic configuration state.

Format

show ipif_ipv6_link_local_auto {<ipif_name 12>}

Description

Use this command to display the link local address automatic configuration state.

Parameters

Parameters	Description
ipif_name	The name of the interface.

Restrictions

None

Examples

To display the link local address automatic configuration state:

```
DGS-3200-10:4#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System           Automatic Link Local Address: Disabled
 IPIF: interface1       Automatic Link Local Address: Enabled

DGS-3200-10:4#
```

32 Auto Config Command List

show autoconfig
enable autoconfig
disable autoconfig

32-1 show autoconfig

Purpose

To display the DHCP auto configuration status.

Format

show autoconfig

Description

This command is used to display the DHCP auto configuration status.

Restrictions

None.

Example

To display the DHCP auto configuration status:

```
DGS-3200-10:4#show autoconfig
Command: show autoconfig


Autoconfig State: Disabled


DGS-3200-10:4#
```

32-2 enable autoconfig

Purpose

To enable DHCP auto configuration.

Format

enable autoconfig

Description

This command is used to enable DHCP auto configuration.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable DHCP auto configuration status:

```
DGS-3200-10:4#enable autoconfig
Command: enable autoconfig

Success.

DGS-3200-10:4#
```

32-3 disable autoconfig

Purpose

To disable DHCP auto configuration.

Format

disable autoconfig

Description

This command is used to disable DHCP auto configuration.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the DHCP auto configuration status:

```
DGS-3200-10:4#disable autoconfig
Command: disable autoconfig

Success.

DGS-3200-10:4#
```

33 Routing Table Command List

create iproute default <ipaddr> {<metric 1-65535>}

delete iproute default

show iproute {<static>}

create ipv6route [default] [<ipif_name 12> <ipv6addr> |<ipv6addr>] {<metric 1-65535>}

delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] | all]

show ipv6route

33-1 create iproute

Purpose

To create a default IP route entry.

Format

create iproute default <ipaddr> {<metric 1-65535>}

Description

This command is used to create a default IP route entry.

Parameters

Parameters	Description
ipaddr	The IP address for the next hop router.
metric	The default setting is 1.That is, the default hop cost is 1.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a static address 10.48.74.121:

```
DGS-3200-10:4#create iproute default 10.48.74.121
Command: create iproute default 10.48.74.121


Success.


DGS-3200-10:4#
```

33-2 delete iproute default

Purpose

To delete a default IP route entry.

Format

delete iproute default

Description

This command is used to delete a default route entry.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a default route from the routing table:

```
DGS-3200-10:4#delete iproute default
Command: delete iproute default


Success.


DGS-3200-10:4#
```

33-3 show iproute

Purpose

To display the switch’s current IP routing table.

Format

show iproute {<static>}

Description

This command is used to display the switch’s current IP routing table.

Parameters

Parameters	Description
<static>	The static address.

Restrictions

None.

Examples

To display the contents of the IP routing table:

```
DGS-3200-10:4#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface     Hops      Protocol
------------------  ---------------  ------------  --------  --------
10.0.0.0/8          0.0.0.0          System        1         Local

Total Entries : 1

DGS-3200-10:4#
```

33-4 create ipv6route

Purpose

To create an IPv6 default route.

Format

create ipv6route [default] [<ipif_name 12> <ipv6addr>| <ipv6addr>]{<metric 1-65535>}

Description

This command is used to create an IPv6 static route. 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.

Parameters

Parameters	Description
default	Specifies the default route.
ipif_name	Specifies the interface for the route.
ipv6addr	Specify the next hop address for this route.
metric	The default setting is 1.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an IPv6 default route:

```
DGS-3200-10:4#create ipv6route default System FEC0::5
Command: create ipv6route default System FEC0::5


Success.


DGS-3200-10:4#
```

33-5 delete ipv6route

Purpose

To delete an IPv6 static route.

Format

delete ipv6route [default] [<ipif_name> <ipv6addr> | <ipv6addr>] | all]

Description

This command is used to delete an IPv6 static route. 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.

Parameters

Parameters	Description
default	Specifies the default route.
ipv6addr	Specify the next hop address for the default route
all	All static created routes will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an IPv6 static route:

```
DGS-3200-10:4#delete ipv6route default System FEC0::5
Command: delete ipv6route default System FEC0::5

Success.

DGS-3200-10:4#
```

33-6 show ipv6route

Purpose

To display IPv6 routes.

Format

show ipv6route

Description

This command is used to display IPv6 routes.

Parameters

None.

Restrictions

None.

Examples

To display an IPv6 route:

```
DGS-3200-10:4#show ipv6route
Command: show ipv6route

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


Total Entries: 1


DGS-3200-10:4#
```

34 ARP Command List

create arpentry <ipaddr> <macaddr>

delete arpentry { <ipaddr> | all }

config arpentry <ipaddr> <macaddr>

config arp_aging time <value 0-65535>

clear arptable

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

34-1 create arpentry

Purpose

To make a static entry in the ARP table.

Format

create arpentry <ipaddr> <macaddr>

Description

This command is used to enter an IP address and the corresponding MAC address into the switch's ARP table.

Parameters

Parameters	Description
ipaddr	The IP address of the end node or station.
macaddr	The MAC address corresponding to the IP address above.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
DGS-3200-10:4#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-3200-10:4#
```

34-2 delete arpentry

Purpose

To delete a static entry into the ARP table.

Format

delete arpentry {<ipaddr> | all}

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** clears the switch's ARP table.

Parameters

Parameters	Description
ipaddr	The IP address of the end node or station.
all	Deletes all ARP entries

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DGS-3200-10:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3200-10:4#
```

34-3 config arpentry

Purpose

To configure a static entry to the ARP table.

Format

config arpentry <ipaddr> <macaddr>

Description

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

Parameters

Parameters	Description
ipaddr	The IP address of the end node or station.
macaddr	The MAC address corresponding to the IP address above.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
DGS-3200-10:4#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-3200-10:4#
```

34-4 config arp_aging time

Purpose

To configure the age-out timer for ARP table entries on the switch.

Format

config arp_aging time <value 0-65535>

Description

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

Parameters

Parameters	Description
value	The ARP age-out time, in minutes. The default is 20. The range is 0 to 65535.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the ARP aging time:

```
DGS-3200-10:4#config arp_aging time 30
Command: config arp_aging time 30


Success.


DGS-3200-10:4#
```

34-5 show arpentry

Purpose

To display the ARP table.

Format

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

Description

This command is used to display the Address Resolution Protocol (ARP) table. You can filter the display by IP address, Interface name, or static entries.

Parameters

Parameters	Description
ipif_name	The name of the IP interface the end node or station for which the ARP table entry was made, resides on.
ipaddr	The IP address of the end node or station.
static	Displays the static entries to the ARP table.
	If no parameter is specified, all ARP entries will be displayed.

Restrictions

None.

Examples

To display the ARP table:

```
DGS-3200-10:4# 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-3200-10:4#
```

34-6 clear arptable

Purpose

To remove dynamic entries from the ARP table.

Format

clear arptable

Description

This command is used to remove dynamic entries from the ARP table. Static ARP entries are not affected.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To remove the dynamic entries from the ARP table:

```
DGS-3200-10:4#clear arptable
Command: clear arptable

Success.

DGS-3200-10:4#
```

35 Loopback Detection Command List

config loopdetect {recover_timer [0 | <value 60-1000000>] | interval <1-32767> | mode [port-based | vlan-based]]
config loopdetect ports [<portlist>| all] state [enable | disable]
enable loopdetect
disable loopdetect
show loopdetect
show loopdetect ports [all | <portlist>]
config loopdetct trap [none | loop_detected | loop_cleared | both]

35-1 config loopdetect

Purpose

To configure the loop-back detection function on the switch.

Format

config loopdetect {recover_timer [0 | <value 60-1000000>] | interval <1-32767> | mode [port-based | vlan-based]}

Description

This command is used to set up the loop-back detection function (LBD) for the entire switch.

Parameters

Parameters	Description
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 valid range is 60 to 1000000. Zero is a special value which means to disable the auto-recovery mechanism, hence, user need to recover the disabled port back manually. Default value of recover_timer is 60.
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. Valid range is 1 to 32767.
mode	Choose the loop-detection operation mode. In the port-based mode , the port will be shut-down (disabled) when detecting loop ; in vlan-based mode , the port can’t process packets of the VLAN that detecting the loop.

Restriction

Only Administrator-level users can issue this command.

Examples

To set a recover time of 0 and an interval of 20 in VLAN-based mode:

```
DGS-3200-10:4# config loopdetect  recover_timer 0 interval 20 vlan-based
Command: config loopdetect  recover_timer 0 interval 20 vlan-based

Success.

DGS-3200-10:4#
```

35-2 config loopdetect ports

Purpose

To configure loop-back detection function for the port on the switch.

Format

config loopdetect ports [<portlist>| all] state [enable | disable]

Description

This command is used to set up the loop-back detection function for the interface on the switch.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured. For setting all ports in the system, you may use the **all** parameter.
all	
state	Allows loop-detect to be enabled or disabled for the ports specified in the port list. The default is disabled.

Restriction

Only Administrator-level users can issue this command.

Examples

To set up loop-back detection:

```
DGS-3200-10:4# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DGS-3200-10:4#
```

35-3 enable loopdetect

Purpose

To globally enable the loop detection function on the switch.

Format

enable loopdetect

Description

This command is used to allow the loop detection function to be globally enabled on the switch. The default value is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable loop detection:

```
DGS-3200-10:4#enable loopdetect
Command: enable loopdetect

Success.

DGS-3200-10:4#
```

35-4 disable loopdetect

Purpose

To globally disable the loop detection function on the switch.

Format

disable loopdetect

Description

This command allows the loop detection function to be globally disabled on the switch. The default value is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable loop detection:

```
DGS-3200-10:4#disable loopdetect
Command: disable loopdetect


Success.


DGS-3200-10:4#
```

35-5 show loopdetect

Purpose

To display the switch's current loop detection configuration.

Format

show loopdetect

Description

This command is used to display the switch's current loop detection configuration.

Parameters

None.

Restrictions

None.

Examples

To display the switch's current loop detection configuration:

```
DGS-3200-10:4#show loopdetect
Command: show loopdetect

 LBD Global Settings
 ------------------------------
 LBD Status                    : Disabled
 LBD Interval                  : 10
 LBD Recover Time              : 60
 LBD Mode                      : Port-Based
 LBD Trap Status               : None

DGS-3200-10:4#
```

35-6 show loopdetect ports

Purpose

To display the switch’s current per-port loop detection configuration.

Format

show loopdetect ports [all | <portlist>]

Description

This command is used to display the switch’s current per-port loop detection configuration and status.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be displayed.
all	System will display port loop detection information for all ports.

Restrictions

None.

Examples

To display the loop detection state of ports 1 to 9 in port-based mode:

```
DGS-3200-10:4#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-3200-10:4#
```

To display loop detection state of ports 1 to 9 under VLAN-based mode:

```
DGS-3200-10:4#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-3200-10:4#
```

35-7 config loopdetect trap

Purpose

To configure the trap mode.

Format

config loopdetect trap [none | loop_detected | loop_cleared | both]

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.

Parameters

Parameters	Description
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-level users can issue this command.

Examples

To configure a trap:

```
DGS-3200-10:4#config loopdetect trap both
Command: config loopdetect trap both


Success.


DGS-3200-10:4#
```

VII. Multicast

The Multicast section includes the following chapters: IGMP Snooping, IGMP Authentication, MLD Snooping, Limited Multicast IP Address, and IGMP Snooping Multicast VLAN (ISM).

36 IGMP Snooping Command List

```
config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> |all] { host_timeout <sec
1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state
[enable|disable] | fast_leave [enable|disable] }

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 1-255> | last_member_query_interval
<sec 1-25> | state [enable|disable] version <value 1-3> }

config router_ports <vlan_name 32> [add|delete]<portlist>

config router_ports_forbidden <vlan_name 32> [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> }

config igmp_snooping data_driven_learning [vlan <vlan_name 32> | vlanid <vidlist> |all] {state
[enable | disable] | aged_out [enable | disable ] }

config igmp_snooping data_ driven _learning max_learned_entry <value 1-256>

clear igmp_snooping data_ driven _group [ all | [vlan <vlan_name 32> | vlanid <vlanid>]
<ipaddress>| all ]]

show router_ports {vlan <vlan_name 32> | vlanid <vlanid_list> } {static |dynamic|forbidden}
```

36-1 config igmp_snooping

Purpose

To configure IGMP snooping on the switch.

Format

config igmp_snooping [vlan_name <vlan_name 32>| vlanid <vlanid_list> |all] { host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state [enable|disable] | fast_leave [enable|disable] }

Description

This command is used to configure IGMP snooping on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which IGMP snooping is to be configured. **all** indicates all VLANs.
host_timeout	Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.
route_timeout	Specifies the maximum amount of time a route will remain in the switch's can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.
leave_timer	Leave timer. The default setting is 2.
state	Enable or 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.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure IGMP snooping:

```
 DGS-3200-10:4#config igmp_snooping default host_timeout 250 state enable
 Command: config igmp_snooping default host_timeout 250 state enable fast_leave
enable

 Success.

 DGS-3200-10:4#
```

36-2 config igmp_snooping querier

Purpose

To configure the the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, the permitted packet loss that guarantees IGMP snooping.

Format

config igmp_snooping querier [vlan_name <vlan_name 32>| vlanid <vlanid_list> |all] { query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable|disable] version <value 1-3> }

Description

This command is used to configure the IGMP snooping querier.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which IGMP snooping querier is to be configured.
query_interval	Specifies the amount of time in seconds between general query transmissions. the default setting is 125 seconds..
max_reponse_time	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: ・ Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). ・ Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). ・ Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. ・ By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy.
last_member_query_interval	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.
state	If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). It 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.
version	Specifies 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 dropped.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the IGMP snooping querier:

```
DGS-3200-10:4#config igmp_snooping querier default query_interval 125 state enable
Command: config igmp_snooping querier default query_interval 125 state enable

Success.

DGS-3200-10:4#
```

36-3 config router_ports

Purpose

To configure ports as router ports.

Format

config router_ports <vlan_name 32> [add|delete] <portlist>

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.

Parameters

Parameters	Description
vlan_name	The name of the VLAN on which the router port resides.
add | delete	Specifies to add or delete the router ports .
portlist	Specifies a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set up static router ports:

```
DGS-3200-10:4#config router_ports default add 1-10
Command: config router_ports default add 1-10


Success.


DGS-3200-10:4#
```

36-4 config router_ports_forbidden

Purpose

To configure ports as forbidden router ports.

Format

config router_ports_forbidden <vlan_name 32> [add|delete] <portlist>

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.

Parameters

Parameters	Description
vlan_name	The name of the VLAN on which the router port resides.
add | delete	Specifies to add or delete the router ports.
portlist	Specifies a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set up port range 1 to 7 to be forbidden router ports of the default VLAN:

```
DGS-3200-10:4#config router_ports_forbidden default add 1-7
Command: config router_ports_forbidden default add 1-7


Success.


DGS-3200-10:4#
```

36-5 enable igmp_snooping

Purpose

To enable IGMP snooping on the switch.

Format

enable igmp_snooping

Description

This command allows you to enable IGMP snooping on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable IGMP snooping on the switch:

```
DGS-3200-10:4#enable igmp_snooping
Command: enable igmp_snooping


Success.


DGS-3200-10:4#
```

36-6 disable igmp_snooping

Purpose

To disable IGMP snooping on the switch.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable IGMP snooping:

```
DGS-3200-10:4#disable igmp_snooping
Command: disable igmp_snooping


Success.


DGS-3200-10:4#
```

36-7 show igmp_snooping

Purpose

To display the current status of IGMP snooping on the switch.

Format

show igmp_snooping {vlan <vlan_name 32> | vlanid <vlanid_list>}

Description

This command is used to display the current IGMP snooping configuration on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which you want to view the IGMP snooping configuration.
	If no parameter is specified, the system will display all current IGMP snooping configuration.

Restrictions

None.

Examples

To show IGMP snooping:

```
DGS-3200-10:4#show igmp_snooping
Command: show igmp_snooping


Data Learn Max Entries      : 56


VLAN  Name                  : default
Query Interval              : 125
Max Response Time           : 10
Robustness Value            : 2
Last Member Query Interval  : 1
Host Timeout                : 260
Router Timeout              : 260
Leave Timer                 : 2
Querier State               : Disabled
Querier Router Behavior     : Non-Querier
State                       : Disabled
Fast Leave                  : Disabled
Version                     : 3
Data Learn State            : Enabled
Data Learn Aged             : Disabled



Total Entries: 1

DGS-3200-10:4#
```

36-8 show igmp_snooping group

Purpose

To display the current IGMP snooping group configuration on the switch.

Format

show igmp_snooping group {vlan <vlan_name 32>| vlanid <vlanid_list>}

Description

This command is used to display the current IGMP snooping group configuration on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which you want to view IGMP snooping group configuration information.
	If no parameter specified, the system will display all current IGMP group snooping configuration of the switch.

Restrictions

None.

Examples

To display IGMP snooping group(s):

```
DGS-3200-10:4#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
 Mode            : EXCLUDE


 Source/Group    : NULL  / 234.54.163.75
 VLAN Name/VID   : default/1
 Member Ports    : 1
 UP Time         : 223
 Expiry Time     : 37
 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     : 0
 Mode            : EXCLUDE
 Source/Group   : 172.16.20.26 / 236.25.213.68
 VLAN Name/VID  : default/1
 Member Ports   : 2
 UP Time        : 222
 Expiry Time    : 38
 Mode           : INCLUDE



 Source/Group   : 172.16.20.27 / 236.25.213.68
 VLAN Name/VID  : default/1
 Member Ports   : 2
 UP Time        : 222
 Expiry Time    : 38
 Mode           : INCLUDE




 Total Entries : 5



DGS-3200-10:4#
```

36-9 config igmp_snooping group data_driven_learning

Purpose

To enable or disable data driven learning of an IGMP snooping group.

Format

config igmp_snooping data_driven_learning [vlan <vlan_name 32> | vlanid <vidlist> |all] {state [enable | disable] | aged_out [enable | disable] }

Description

This command is used to enable or disable data driven learning of an IGMP snooping group. When data-driven learning is enabled for the VLAN, the switch receives the IP multicast traffic on this VLAN, and an IGMP snooping group is created. That is, the learning of an entry is not activated by IGMP membership registration, but activated by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to ageout or to ageout by the aging timer.

When data driven learning is enabled, the multicast filtering mode for all ports is ignored. This means multicast packets will be flooded. If a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. Thus, the aging out mechanism will follow the rules of an ordinary IGMP snooping entry.

Parameters

Parameters	Description
vlan_name	Specifies the VLAN name to be configured.
state	Specifies whether to enable or disable the data driven learning of an IGMP snooping group. This is enabled by default.
aged_out	Enable or disable the aging on the entry. This is disabled by default.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable data driven learning of an IGMP snooping group on a default VLAN:

```
DGS-3200-10:4# config igmp_snooping data_driven_learning vlan default state enable
Command: config igmp_snooping data_driven_learning vlan default state enable

Success.

DGS-3200-10:4#
```

36-10 config igmp_snooping data_driven_learning max_learned_entry

Purpose

To configure the maximum number of groups that can be learned by the data driven mechanism.

Format

config igmp_snooping data_driven_learning max_learned_entry <value 1-256>

Description

This command is used to configure the maximum number of groups that can be learned by the data driven mechanism. When the table is full, the system will stop learning new data-driven groups. Traffic for the new groups will be dropped.

Parameters

Parameters	Description
max_learned_entry	Specifies the maximum number of groups that can be learned by the data driven mechanism. The default is 56.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4#config igmp_snooping data_ driven_learning max_learned_entry 50
Command: config igmp_snooping data_ driven_learning max_learned_entry 50


Success.


DGS-3200-10:4#
```

36-11 clear igmp_snooping data_driven_group

Purpose

To delete the IGMP snooping group learned by the data driven mechanism.

Format

clear igmp_snooping data_ driven _group [all | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [<ipaddress>| all]]

Description

This command is used to delete the IGMP snooping group learned by the data driven mechanism.

Parameters

Parameters	Description
all	Delete all entries learned by the data driven mechanism.
vlan_name	Specifies the VLAN name.
group	Delete the specific entry learned by the data driven mechanism.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete all the groups learned by the data-driven mechanism:

```
DGS-3200-10:4#clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all


Success.


DGS-3200-10:4#
```

36-12 show router_ports

Purpose

To display the currently configured router ports on the switch.

Format

show router_ports {vlan <vlan_name 32>| vlanid <vlanid_list>}{static|dynamic|forbidden}

Description

This command is used to display the currently configured router ports on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN on which the router port resides.
static	Displays router ports that have been statically configured.
dynamic	Displays router ports that have been dynamically registered.
forbidden	Displays forbidden router ports that have been statically configured.
	If no parameter is specified, the system will display all currently configured router ports on the switch.

Restrictions

None.

Examples

To display the router ports:

```
DGS-3200-10:4#show router_ports
Command: show router_ports

VLAN Name               : default
Static router port      : 1-7
Dynamic router port     :
Forbidden router port   :

VLAN Name               : vlan2
Static router port      :
Dynamic router port     :
Forbidden router port   :

Total Entries : 2

DGS-3200-10:4#
```

37 IGMP Authentication Command List

config igmp access_authentication ports [all|<portlist>] state [enable|disable]

show igmp access_authentication ports [all|<portlist>]

37-1 config igmp access_authentication ports

Purpose

To configure IGMP authentication port status.

Format

config igmp access_authentication ports [all|<portlist>] state [enable|disable]

Description

This command is used to enable or disable IGMP authentication for the specified port. When the command is enabled, and the switch receives an IGMP join request, the switch will send the access request to the RADIUS server to do the authentication.

Parameters

Parameters	Description
ports	Specifies a range of ports to be configured.
state	Enable or disable the RADIUS authentication function on the specified ports.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable IGMP authentication for all ports:

```
DGS-3200-10:4#config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable

Success.

DGS-3200-10:4#
```

37-2 show igmp access_authentication ports

Purpose

To display the current IGMP authentication configuration.

Format

show igmp access_authentication ports {<portlist>}

Description

This command is used to display the current IGMP authentication configuration.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be displayed. When port list is not specified, information for all ports will be displayed.

Restrictions

None.

Example

To display IGMP Access Control status for ports 1 to 4:

```
DGS-3200-10:4# show igmp access_authentication ports 1-4

Command: show igmp access_authentication ports 1-4

Port        State

-----       ---------

 1          Enabled

 2          Disabled

 3          Disabled

 4          Enabled



DGS-3200-10:4#
```

38 MLD Snooping Command List

config mld_snooping [<vlan_name 32> | vlanid <vlanid_list> |all] { node_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | done_timer <sec 1-16711450> | state [enable|disable] | fast_done [enable|disable] }

config mld_snooping querier [<vlan_name 32> | vlanid <vlanid_list> |all] { query_interval <sec 1-65535> |max_response_time <sec 1-25>| robustness_variable <value 1-255> | last_listener_query_interval <sec 1-25> | state [enable|disable] | version <value 1-2>} }

config mld_snooping mrouter_ports <vlan_name 32> [add|delete]<portlist>

config mld_snooping mrouter_ports_forbidden <vlan_name 32> [add|delete]<portlist>

enable mld_snooping

disable mld_snooping

show mld_snooping {vlan <vlan_name 32>| vlanid <vlanid >}

show mld_snooping group {vlan <vlan_name 32>| vlanid <vlanid > }

show mld_snooping mrouter_ports {vlan <vlan_name 32>| vlanid <vlanid_list>}
{ [static|dynamic|forbidden]}

38-1 config mld_snooping

Purpose

To configure MLD snooping on the switch.

Format

config mld_snooping [<vlan_name 32>| vlanid <vlanid_list> |all] { node_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | done_timer <sec 1-16711450> | state [enable|disable] | fast_done [enable|disable] }

Description

This command is used to configure MLD snooping on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which MLD snooping is to be configured. **all** indicates all VLANs.
node_timeout	Specifies the amount of time that must pass before a link node is considered to be not a listener anymore. The default is 260 seconds.
router_timeout	Specifies the maximum amount of time a router will remain the switch's can be a listener of a multicast group without the switch receiving a node listener report. The default is 260 seconds.

done_timer	The done timer. The default setting is 2.
state	**enable** or **disable** MLD snooping for the chosen VLAN.
fast_done	**enable** or **disable** the MLD snooping fast done function. If enabled, the membership is immediately removed when the system receives the MLD done message.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure MLD snooping:

```
DGS-3200-10:4#config mld_snooping default node_timeout 250 state enable
Command: config mld_snooping default node_timeout 250 state enable


Success.


DGS-3200-10:4#
```

38-2 config mld_snooping querier

Purpose

To configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from listeners, the permitted packet loss that guarantees MLD snooping.

Format

config mld_snooping querier [<vlan_name 32>| vlanid <vlanid_list>| |all] { query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_listener_query_interval <sec 1-25> | state [enable|disable] | version <value 1-2> }

Description

This command is used to configure the MLD snooping querier.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which MLD snooping querier is to be configured.
query_interval	Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.
max_reponse_time	The maximum time in seconds to wait for reports from listeners. 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: • Group listener interval—Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval). • Last listener query count—Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy.
last_listener_query_interval	The maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group.
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.
version <value 1-2>	Specifies 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 dropped.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the MLD snooping querier:

```
DGS-3200-10:4#config mld_snooping querier default query_interval 125 state enable
Command: config mld_snooping querier default query_interval 125 state enable

Success.

DGS-3200-10:4#
```

38-3 config mld_snooping mrouter_ports

Purpose

To configure ports as router ports.

Format

config mld_snooping mrouter_ports <vlan_name 32> [add|delete] <portlist>

Description

This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.

Parameters

Parameters	Description
vlan_name	The name of the VLAN on which the router port resides.
add | delete	Specifies to add or delete the router ports.
portlist	Specifies a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Example

To set up static router ports:

```
DGS-3200-10:4#config mld_snooping mrouter_ports default add 1-10
Command: config mld_snooping mrouter_ports default add 1-10


Success.


DGS-3200-10:4#
```

38-4 config mld_snooping mrouter_ports_forbidden

Purpose

To configure ports as forbidden router ports.

Format

config mld_snooping mrouter_ports_forbidden <vlan_name 32> [add|delete] <portlist>

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.

Parameters

Parameters	Description
vlan_name	The name of the VLAN on which the router port resides.
add | delete	Specifies to add or delete the router ports.
portlist	Specifies a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Example

To set up static router ports:

```
DGS-3200-10:4#config mld_snooping mrouter_ports_forbidden default add 1-10
Command: config mld_snooping mrouter_ports_forbidden default add 1-10


Success.


DGS-3200-10:4#
```

38-5 enable mld_snooping

Purpose

To enable MLD snooping on the switch.

Format

enable mld_snooping

Description

This command is used to enable MLD snooping on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable MLD snooping on the switch:

```
DGS-3200-10:4#enable mld_snooping
Command: enable mld_snooping


Success.


DGS-3200-10:4#
```

38-6 disable mld_snooping

Purpose

To disable MLD snooping on the switch.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable MLD snooping on the switch:

```
DGS-3200-10:4#disable mld_snooping
Command: disable mld_snooping


Success.


DGS-3200-10:4#
```

38-7 show mld_snooping

Purpose

To display the current status of MLD snooping on the switch.

Format

show mld_snooping {vlan <vlan_name 32>| vlanid <vlanid_list> }

Description

This command is used to display the current MLD snooping configuration on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which you want to view the MLD snooping configuration.
	If no parameter is specified, the system will display all current MLD snooping configurations.

Restrictions

None.

Example

To display MLD snooping:

```
DGS-3200-10:4#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
Node Timeout                  : 260
Router Timeout                : 260
Done Timer                    : 2
Querier State                 : Disabled
Querier Router Behavior       : Non-Querier
State                         : Disabled
Fast Done                     : Disabled
 Version                      : 2

Total Entries: 1

DGS-3200-10:4#
```

38-8 show mld_snooping group

Purpose

To display the current MLD snooping group configuration on the switch.

Format

show mld_snooping group {vlan <vlan_name 32>| vlanid <vlanid_list>}

Description

This command is used to display the current MLD snooping group configuration on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which you want to view MLD snooping group configuration information.
	If no parameter is specified, the system will display all current MLD group snooping configuration of the switch.

Restrictions

None.

Examples

To show the MLD snooping group:

```
DGS-3200-10:4#show mld_snooping group
Command: show mld_snooping group

Source/Group      :   2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID     :   default/1
Member Ports      :   1-2
Filter Mode       :   INCLUDE

Source/Group      :   2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID     :   default/1
Member Ports      :   3
Filter Mode       :   EXCLUDE

Source/Group      :   NULL/FF0E::100:0:0:21
VLAN Name/VID     :   default/1
Member Ports      :   4-5
Filter Mode       :   EXCLUDE
```

```
Total Entries :  3

DGS-3200-10:4#
```

38-9 show mld_snooping mrouter_ports

Purpose

To display the currently configured router ports on the switch.

Format

show mld_snooping mrouter_ports {vlan <vlan_name 32>| vlanid <vlanid_list>}{[static|dynamic|forbidden}}

Description

This command is used to display the currently configured router ports on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN on which the router port resides.
static	Displays router ports that have been statically configured.
dynamic	Displays router ports that have been dynamically configured.
forbidden	Displays forbidden router ports that have been statically configured.
	If no parameter is specified, the system will display all currently configured router ports on the switch.

Restrictions

None.

Example

To display router ports:

```
DGS-3200-10:4#show mld_snooping mrouter_ports
Command: show mld_snooping mrouter_ports

VLAN Name               : default
Static mrouter port     : 1-10
Dynamic mrouter port    :
Forbidden mrouter port  :

VLAN Name               : vlan2
Static mrouter port     :
Dynamic mrouter port    :
Forbidden mrouter port  :

Total Entries : 2

DGS-3200-10:4#
```

39 Limited Multicast IP Address Command List

create mcast_filter_profile profile_id <value 1-24> profile_name <name>

config mcast_filter_profile [profile_id < value 1-24>| profile_name <name>] { profile_name <name> | [add | delete] <mcast_address_list>}

delete mcast_filter_profile profile_id [<value 1-24> | all]

delete mcast_filter_profile profile_name <name>

show mcast_filter_profile { profile_id <value 1-24>}

config limited_multicast_addr [ports <portlist>] {[add | delete] [profile_id <value 1-24> | profile_name <name>] | access [permit | deny]}

show limited_multicast_addr { ports <portlist> }

config max_mcast_group ports {<portlist>} max_group [<value 1-256>]

show max_mcast_group ports {ports <portlist>}

39-1 create mcast_filter_profile

Purpose

To create a multicast address profile.

Format

create mcast_filter_profile profile_id <value 1-24> <name>

Description

This command is used to configure a multicast address profile. Mutliple ranges of multicast addresses can be defined in the profile.

Parameters

Parameters	Description
profile_id	ID of the profile. Range is 1 to 24.
name	Provides a meaningful description for the profile.

Restrictions

Only Administrator-level users can issue this command.

Examples

```
DGS-3200-10:4# create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD


Success.


DGS-3200-10:4#
```

39-2 config mcast_filter_profile

Purpose

To add or delete a range of multicast addresses to the profile.

Format

config mcast_filter_profile [profile_id < value 1-24>| profile_name <name>] { profile_name <name> | [add | delete] <mcast_address_list>}

Description

This command is used to add or delete a range of previously defined multicast IP addresses.

Parameters

Parameters	Description
profile_id	The ID of the profile.
profile_name	Provides a meaningful description for the profile.
mcast_address_list	List of the multicast addresses to be put in the profile. You can either specifiy a single multicast IP address or a range of multicast addresses using a hyphen.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a range of multicast addresses to a profile:

```
DGS-3200-10:4# config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.1
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.1


Success.


DGS-3200-10:4#
```

39-3 delete mcast_filter_profile

Purpose

To delete a multicast address profile.

Format

delete mcast_filter_profile profile_id [<value 1-24> | all]

Description

This command is used to delete a multicast address profile

Parameters

Parameters	Description
profile_id	The ID of the profile
all	All multicast address profiles will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a multicast profile:

```
DGS-3200-10:4# delete mcast_filter_profile profile_id  3
Command: delete mcast_filter_profile profile_id  3


Success.


DGS-3200-10:4#
```

39-4 show mcast_filter_profile

Purpose

To display defined multicast address profiles.

Format

show mcast_filter_profile { profile_id <value 1-24>}

Description

This command is used to display defined multicast address profiles.

Parameters

Parameters	Description
profile_id	The ID of the profile. If not specified, all profiles will be displayed.

Restrictions

None.

Examples

To display defined multicast address profiles:

```
DGS-3200-10:4#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-3200-10:4#
```

39-5 config limited_multicast_addr

Purpose

To configure the multicast address filtering function on a port.

Format

config limited_multicast_addr   ports [<portlist> | vlanid <vlanid_list >] {[add | delete] profile_id <value 1-24> | access [permit | deny]}

Description

This command is used to configure the multicast address filtering function on a port or VLAN. When there are no profiles specified with a port or VLAN, the limited function is not effective. When the function is configured on a port, it limits the multicast group operated by the IGMP snooping function and layer 3 function. When the function is configured on a VLAN, it limits the multicast group operated by the IGMP layer 3 function.

Parameters

Parameters	Description
<portlist>	A range of ports to config the multicast address filtering function.
add	Add a multicast address profile to a port.
delete	Delete a multicast address profile to a port.
profile_id	A profile to be added to or deleted from the port.
permit	Specifies that the packets that match the addresses defined in the profiles will be permitted. The default mode is **permit**.
deny	Specifies that the packets that match the addresses defined in the profiles will be denied.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure ports 1 and 3 to set the multicast address profile 2:

```
DGS-3200-10:4# 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-3200-10:4#
```

39-6 show limited multicast addr

Purpose

To display a per-port Limited IP multicast address range.

Format

show limited_multicast_addr { ports <portlist> }

Description

This command is used to display a multicast address range by ports or by VLANs. When the function is configured on a port, it limits the multicast groups operated by the IGMP snooping function and layer 3 function. When the function is configured on a VLAN, it limits the multicast groups operated by the IGMP layer 3 function.

Parameters

Parameters	Description
<portlist>	A range of ports to show the limited multicast address configuration.

Restrictions

None.

Examples

To display a limited multicast address range for ports 1 and 3:

```
DGS-3200-10:4#show limited_multicast_addr 1,3
Command: show limited_multicast_addr 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-3200-10:4#
```

39-7 config max_mcast_group

Purpose

To configure the maximum number of multicast groups a port can join.

Format

config max_mcast_group ports [<portlist>] max_group [<value 1-256>]

Description

This command is used to configure the maximum number of multicast groups a port can join.

Parameters

Parameters	Description
<portlist>	A range of ports to config the max_mcast_group.
max_group	Specifies the maximum number of the multicast groups. The range is from 1 to 256 or infinite. Infinite is the default setting.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a maximum of 200 mulitcast groups for ports 1 and 3:

```
DGS-3200-10:4# config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DGS-3200-10:4#
```

39-8 show max_mcast_group

Purpose

To display the maximum number of multicast groups that a port can join.

Format

show max_mcast_group ports {<portlist>}

Description

This command is used to display the maximum number of multicast groups that a port can join.

Parameters

Parameters	Description
<portlist>	A range of ports to display the max number of multicast groups.

Restrictions

None.

Examples

To display the maximum number of multicast groups that port 3 can join:

```
DGS-3200-10:4# show max_mcast_group ports 1
Command: show max_mcast_group ports 1

Max Multicast Filter Group:
 Port     MaxMcastGroup
 -----    -------------
 1        256

DGS-3200-10:4#
```

40 IGMP Snooping Multicast VLAN (ISM) Command List

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | source_port <portlist> |tag_member_port <portlist>]| state [enable|disable] |replace_source_ip <ipaddr>}
create igmp_snooping multicast_group_profile <profile_name 1-32>
config igmp_snooping multicast_ group_profile <profile_name 1-32> [add | delete] <mcast_address_list>
delete igmp_snooping multicast_ group_profile [<profile_name 1-32>|all]
show igmp_snooping multicast_ 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>}

40-1 create multicast_vlan

Purpose

To create a multicast VLAN.

Format

create [igmp_snooping | mld_snooping] multicast_vlan <vlan_name 32> <vlanid 2-4094>

Description

This command is used to create a multicast VLAN. Multiple multicast VLANs can be configured. The restriction on the number of multicast VLANs for IGMP snooping or MLD snooping are mutually exclusive. The ISM VLANs being created can not exist in the 1Q VLAN database. Multiple ISM VLANs can be created. The ISM VLAN snooping function co-exists with the 1Q VLAN snooping function..

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping.
vlan_name	The name of the multicast VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.

vlanid	The VLAN ID of the multicast VLAN to be created. The range is from 2 to 4094.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an IGMP snooping multicast VLAN called “mv1 2”:

```
DGS-3200-10:4# create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2

Success.

DGS-3200-10:4#
```

40-2 config multicast_vlan

Purpose

To configure the parameters of a specific multicast VLAN.

Format

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | source_port <portlist> |tag_member_port <portlist>]| state [enable|disable] |replace_source_ip <ipaddr>}

Description

This command is used to add member ports and add source ports to a port list. The member port will automatically become an untagged member of the multicast VLAN, and the source port will automatically become a tagged member of the multicast VLAN. If the add or delete is not specified, the new port-list will replace the previous port-list. The member port list and source port list can not overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN. The multicast VLAN must be created first, before configuration.

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping.
vlan_name	The name of the multicast VLAN to be configured. Each multicast VLAN is given a name that can be up to 32 characters.
member_port	A range of member ports to add to the multicast VLAN. They will

	become the untagged member ports of the ISM VLAN.
tag_member_port	Specifies the tagged member port of the ISM VLAN.
source_port	A range of member ports to add to the multicast VLAN.
state	Enable or 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 not be replaced.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure an IGMP snooping multicast VLAN:

```
DGS-3200-10:4# config igmp_snooping multicast_vlan v1 member_port 1,3
source_port 2 state enable
Command: config igmp_snooping multicast_vlan v1 member_port 1,3 source_port 2
state enable

Success.

DGS-3200-10:4#
```

40-3 create multicast_group_profile

Purpose

To create a multicast group profile on the switch.

Format

create igmp_snooping multicast_group_profile <profile_name 1-32>

Description

This command is used to create a multicast group profile. The profile name must be unique, whether being used for IGMP snooping or MLD snooping.

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping.
profile_name	Specifies the multicast VLAN profile name. The maximum length is 32 characters.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a multicast group profile:

```
DGS-3200-10:4#create igmp_snooping multicast_group_profile Knicks
Command: create igmp_snooping multicast_group_profile Knicks


Success.


DGS-3200-10:4#
```

40-4 config multicast_group_profile

Purpose

Used to configure an IGMP snooping multicast group profile on the switch and to add or delete multicast addresses for the profile.

Format

config igmp_snooping multicast_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

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.

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping.
profile_id	Specifies the profile ID, from 1 to 16

profile_name	Specifies the multicast VLAN profile name. The maximum length is 32 characters.
add|delete	Add or delete a multicast address list to or from this multicast VLAN profile. The multicast address list can be continuous single multicast addresses, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, or a multicast address range, such as 225.1.1.1-225.2.2.2, or both of them, such as 225.1.1.1, 225.1.1.18-225.1.1.20.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a multicast address to a profile named “Knicks”:

```
DGS-3200-10:4#config igmp_snooping multicast_group_profile Knicks add
225.1.1.1, 225.1.1.10-225.1.1.20
Command: config igmp_snooping multicast_group_profile Knicks add 225.1.1.1,
225.1.1.10-225.1.1.20


Success.


DGS-3200-10:4#
```

40-5 delete multicast_group_profile

Purpose

To delete an existing IGMP snooping multicast group profile.

Format

delete igmp_snooping multicast_group_profile [<profile_name 1-32>|all]

Description

This command is used to delete an existing IGMP snooping multicast group profile.

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping.
profile_name	Specifies the multicast VLAN profile name. The maximum length is 32 characters.
all	Specifies to delete all the multicast VLAN profiles.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a multicast group profile named “Knicks”:

```
DGS-3200-10:4#delete igmp_snooping multicast_group_profile Knicks
Command: delete igmp_snooping multicast_group_profile Knicks


Success.


DGS-3200-10:4#
```

40-6 show multicast_group_profile

Purpose

To display an IGMP snooping multicast group profile.

Format

show igmp_snooping multicast_group_profile {< profile_name 1-32>}

Description

This command is used to display an IGMP snooping multicast group profile.

Parameters

Parameters	Description
profile_name	Specifies the multicast VLAN profile name. The maximum length is 32 characters.

Restrictions

None.

Examples

To display a profile setting:

```
DGS-3200-10:4#show igmp_snooping multicast_group_profile

Command: show igmp_snooping multicast_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-3200-10:4#
```

40-7 config multicast_vlan_group

Purpose

To configure the multicast group which will be learned with the specific multicast VLAN.

Format

config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

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.

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping.
vlan_name	The name of the multicast VLAN to be configured. Each multicast

	VLAN is given a name that can be up to 32 characters.
add	Used to associate a profile to a multicast VLAN.
delete	Used to de-associate a profile from a multicast VLAN.
profile_name	Specifies the multicast vlan profile name. The maximum length is 32 characters.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a profile to a multicast VLAN:

```
DGS-3200-10:4# 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-3200-10:4#
```

40-8 delete multicast_vlan

Purpose

To delete a multicast VLAN.

Format

delete igmp_snooping multicast_vlan <vlan_name 32>

Description

This command is used to delete a multicast VLAN.

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping
vlan_name	The name of the multicast VLAN to be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an IGMP snooping multicast VLAN:

```
DGS-3200-10:4# delete igmp_snooping multicast_vlan v1

Command: delete igmp_snooping multicast_vlan v1


Success.


DGS-3200-10:4#
```

40-9 enable multicast_vlan

Purpose

To enable the multicast VLAN function.

Format

enable igmp_snooping multicast_vlan

Description

This command is used to control the multicast VLAN function. The command **enable igmp_snooping** controls the ordinary IGMP snooping function. By default, the multicast VLAN is disabled.

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable IGMP snooping multicast VLAN:

```
DGS-3200-10:4# enable igmp_snooping multicast_vlan

Command: enable igmp_snooping multicast_vlan


Success.


DGS-3200-10:4#
```

40-10 disable multicast_vlan

Purpose

To disable the multicast VLAN function.

Format

disable igmp_snooping multicast_vlan

Description

This command is used to disable multicast VLAN.

Parameters

Parameters	Description
igmp_snooping	Specifies to configure for IGMP snooping.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable IGMP snooping multicast VLAN:

```
DGS-3200-10:4# disable igmp_snooping multicast_vlan

Command: disable igmp_snooping multicast_vlan



Success.



DGS-3200-10:4#
```

40-11 show multicast_vlan

Purpose

To display multicast VLAN information.

Format

show igmp_snooping multicast_vlan {<vlan_name 32>}

Description

This command is used to display multicast VLAN information.

Parameters

Parameters	Description
vlan_name	The name of the multicast VLAN to be shown.

Restrictions

None.

Examples

To display IGMP snooping multicast VLAN information:

```
DGS-3200-10:4#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

ISM VLAN Global State    : Enabled

VLAN Name                 : mv1
VID                       : 2

Member(Untagged) Ports   : 1,3
Tagged Member Ports      : 2
Source Ports              : 4
Status                    : Enabled
Replace Source IP        : 10.1.1.100

DGS-3200-10:4#
```

VIII. Security

The Security section includes the following chapters: 802.1X, Access Authentication Control, SSL, SSH, IP-MAC-Port Binding (IMPB), Web-based Access Control, MAC-based Access Control, JWAC, Multiple Authentication, and Filter.

41 802.1X Command List

```
enable 802.1x
disable 802.1x
create 802.1x user <username 15>
delete 802.1x user <username 15>
show 802.1x user
config 802.1x auth_protocol [local|radius_eap]
show 802.1x [auth_state | auth_configuration] {ports [<portlist|all>]}
config 802.1x capability ports [<portlist>|all] [authenticator|none]
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> | enable_reauth [enable|disable]}]
config 802.1x auth_mode [port_based |mac_based]
config 802.1x init [port_based ports [<portlist|all>] |mac_based ports [<portlist>|all] {mac_address <macaddr>}]
config 802.1x reauth [port_based ports [<portlist|all>] |mac_based ports [<portlist>|all] {mac_address <macaddr>}]
create 802.1x guest_vlan {<vlan_name 32>}
delete 802.1x guest_vlan {<vlan_name 32>}
config 802.1x guest_vlan ports [<portlist>|all] state [enable | disable]
show 802.1x guest_vlan
config radius add <server_index 1-3> [<server_ip> | <ipv6addr> ] key <passwd 32> [ default | {auth_port<udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <int 1-255> | retransmit <int 1-255>} ]
config radius delete <server_index 1-3>
config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr> ] |key <passwd 32> | auth_port <udp_port_number> | acct_port <udp_port_number> | timeout <int 1-255> | retransmit <int 1-255>}
show radius
```

show auth_statistics {ports [<portlist>|all]}

show auth_diagnostics { ports [<portlist>|all]}

show auth_session_statistics {ports [<portlist>|all]}

show auth_client

show acct_client

41-1 enable 802.1x

Purpose

To enable the 802.1x function.

Format

enable 802.1x

Description

This command is used to enable the 802.1x function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the 802.1x function:

```
DGS-3200-10:4#enable 802.1x
Command: enable 802.1x


Success.


DGS-3200-10:4#
```

41-2 disable 802.1x

Purpose

To disable the 802.1x function.

Format

disable 802.1x

Description

This command is used to disable the 802.1x function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the 802.1x function:

```
DGS-3200-10:4#disable 802.1x
Command: disable 802.1x


Success.


DGS-3200-10:4#
```

41-3 create 802.1x user

Purpose

To create the 802.1x user.

Format

create 802.1x user <username 15>

Description

This command is used to create an 802.1x user.

Parameters

Parameters	Description
username	Specifies adding a user name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a user named “ctsnow”.

```
DGS-3200-10:4#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-3200-10:4#
```

41-4 delete 802.1x user

Purpose

To delete an 802.1x user.

Format

delete 802.1x user <username 15>

Description

This command is used to delete a specified user.

Parameters

Parameters	Description
username	Specifies deleting a user name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete the user named “Tiberius”.

```
DGS-3200-10:4#delete 802.1x user Tiberius
Command: delete 802.1x user Tiberius

Success.

DGS-3200-10:4#
```

41-5 show 802.1x user

Purpose

To display the 802.1x user.

Format

show 802.1x user

Description

This command is used to display 802.1x user account information.

Parameters

None.

Restrictions

None.

Examples

To display 802.1x user information:

```
DGS-3200-10:4#show 802.1x user
Command: show 802.1x user


Current Accounts:
UserName          Password
---------------  ------------
ctsnow            gallinari


Total Entries : 1


DGS-3200-10:4#
```

41-6 config 802.1x auth_protocol

Purpose

To configure the 802.1x authentication protocol

Format

config 802.1x auth_protocol [local|radius_eap]

Description

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

Parameters

Parameters	Description
local	Specifies the auth protocol as local.
radius_eap	Specifies the auth protocol as RADIUS EAP

Restrictions

Only Administrator-level users can issue this command.

Examples

To config the 802.1x RADIUS EAP:

```
DGS-3200-10:4#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap


Success.


DGS-3200-10:4#
```

41-7 show 802.1x

Purpose

To display the 802.1x state or configurations.

Format

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

Description

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

Parameters

Parameters	Description
auth_state	Used to display 802.1x authentication state machine of some or all ports
auth_configuration	Used to display 802.1x configurations of some or all ports.
portlist	Specifies a range of ports to be displayed.
all	All ports.

Restrictions

None.

Examples

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

```
DGS-3200-10:4# show 802.1x auth_state ports 1-5
Command: show 802.1x auth_state ports 1-5

Port    Auth PAE State  Backend State  Port Status
------  --------------  -------------  ------------
1     ForceAuth       Success        Authorized
2     ForceAuth       Success        Authorized
3     ForceAuth       Success        Authorized
4     ForceAuth       Success        Authorized
5     ForceAuth       Success        Authorized

DGS-3200-10:4#
```

To display the 802.1x configuration for port 1:

```
DGS-3200-10:4# show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X                  : Enabled
Authentication Mode     : Port_based
Authentication Protocol : Radius_Eap

Port number    : 1
Capability     : None
AdminCrlDir    : Both
OpenCrlDir     : Both
Port Control   : Auto
QuietPeriod    : 60    sec
TxPeriod       : 30    sec
SuppTimeout    : 30    sec
ServerTimeout  : 30    sec
MaxReq         : 2     times
ReAuthPeriod   : 3600  sec
ReAuthenticate : Disabled

DGS-3200-10:4#
```

41-8 config 802.1x capability

Purpose

To configure port capability.

Format

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

Description

This command is used to configure port capability.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured.
all	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	Allows the flow of PDUs via the port.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure port capability:

```
DGS-3200-10:4#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator


Success.


DGS-3200-10:4#
```

41-9 config 802.1x auth_parameter

Purpose

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>|enable_reauth [enable|disable]}]

Description

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

Parameters

Parameters	Description	
portlist	Specifies a range of ports to be configured.	
all	All ports.	
default	Sets all parameter to be default value.	
direction	Sets the direction of access control .	
	both	For bidirectional access control.
	in	For ingress access control.[0] Note: The **in** option is not supported in the present firmware release.
port_control	You can force a specific port to be unconditionally authorized or unauthorized by setting the the parameter of **port_control** to be **force_authorized** or **force_unauthorized**. Besides, the controlled port will reflect the outcome of authentication if **port_control** is **auto**.	
	force_authorized	The port transmits and receives normal traffic without 802.1X-based authentication of the client.
	auto	The port begins in the unauthorized state, and relays authentication messages between the client and the authentication server.
	force_unauthorized	The port will remain in the unauthorized state, ignoring all attempts by the client to authenticate.
quiet_period	It is the initialization value of the quietWhile timer. The default value is 60 s and can be any value from 0 to 65535.	
tx_period	It is the initialization value of the txWhen timer. The default value is 30 s and can be any value from 1 to 65535.	
supp_timeout	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.	
server_timeout	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.	
max_req	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.	
reauth_period	Its a nonzero number of seconds, which is used to be the re-authentication timer. The default value is 3600.	

enable_reauth	You can enable or disable the re-authentication mechanism for a specific port.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4# config 802.1x auth_parameter ports 1:1-1:20 direction both
Command: config 802.1x auth_parameter ports 1:1-1:20 direction both


Success.


DGS-3200-10:4#
```

41-10 config 802.1x auth_mode

Purpose

To configure 802.1x authentication mode.

Format

config 802.1x auth_mode [port_based |mac_based]

Description

This command is used to configure the authentication mode.

Parameters

Parameters	Description
port_based	Used to configure authentication in port-based mode.
mac_based	To initialize ports in host-based 802.1X mode, the user must first enable the 802.1X MAC-based setting.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the authentication mode:

```
DGS-3200-10:4#config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based


Success.


DGS-3200-10:4#
```

41-11 config 802.1x init

Purpose

To initialize the authentication state machine of some or all ports.

Format

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

Description

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

Parameters

Parameters	Description
port_based	Used to configure authentication in port-based mode.
mac_based	To configure authentication in host-based 802.1X mode, the user first must enable the 802.1X MAC-based setting.
portlist	Specifies a range of ports to be configured.
all	All ports.
mac_address	The MAC address of the host.

Restrictions

Only Administrator-level users can issue this command.

Examples

To initialize the authentication state machine of some or all:

```
DGS-3200-10:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3200-10:4#
```

41-12 config 802.1x reauth

Purpose

To reauthenticate the device connected with the port.

Format

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

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.

Parameters

Parameters	Description
port_based	The switch passes data based on its authenticated port.
mac_based	The switch passes data based on the MAC address of authenticated RADIUS client.
portlist	Specifies a range of ports to be configured.
all	All ports.
mac_address	The MAC address of the authenticated RADIUS client.

.

Restrictions

Only Administrator-level users can issue this command.

Examples

To reauthenticate the device connected with the port:

```
DGS-3200-10:4# config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DGS-3200-10:4#
```

41-13 create 802.1x guest_vlan

Purpose

To assign a static VLAN to be a guest VLAN.

Format

create 802.1x guest_vlan {<vlan_name 32>}

Description

This command is used to assign a static VLAN to be a guest VLAN.

Parameter

Parameters	Description
vlan_name 32	Specify the static VLAN to be a guest VLAN.

Restrictions

Only Administrator-level users can issue this command. 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.

Example

To assign a static VLAN to be a guest VLAN:

```
DGS-3200-10:4# create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN


Success.


DGS-3200-10:4#
```

41-14 delete 802.1x guest_vlan

Purpose

To delete a guest VLAN configuration.

Format

delete 802.1x guest_vlan {<vlan_name 32>}

Description

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

Parameter

Parameters	Description
vlan_name 32	The guest VLAN name.

Restrictions

Only Administrator-level users can issue this command. All ports which are enabled as guest VLAN will return to the original VLAN after the guest VLAN is deleted.

Example

To delete a guest VLAN configuration:

```
DGS-3200-10:4# delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN


Success.


DGS-3200-10:4#
```

41-15 config 802.1x guest vlan

Purpose

To configure a guest VLAN setting.

Format

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

Description

This command is used to configure a guest VLAN setting.

Parameter

Parameters	Description
ports	A range of ports to enable or disable the guest VLAN function
all	All ports.
state	Specify the guest VLAN port state of the configured ports. **enable**: join to the guest VLAN. **disable**: remove from guest VLAN.

Restrictions

Only Administrator-level users can issue this command. If the specific port state is changed from the enabled state to the disabled state, this port will move to its original VLAN.

Example

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

```
DGS-3200-10:4# config 802.1x guest_vlan ports 1-8 state enable
Command: config 802.1x guest_vlan ports 1-8 state enable


Warning! GVRP of the ports were disable !


Success.


DGS-3200-10:4#
```

41-16 show 802.1x guest vlan

Purpose

To display the guest VLAN setting.

Format

show 802.1x guest _vlan

Description

This command is used to display guest VLAN information.

Parameter

None.

Restrictions

None.

Example

To display guest VLAN information:

```
DGS-3200-10:4#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

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

DGS-3200-10:4#
```

41-17 config radius add

Purpose

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 <passwd 32> [default | { auth_port<udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>| timeout <int 1-255> | retransmit <int 1-255>}]

Description

This command is used to add a new RADIUS server.

Parameters

Parameters	Description
server_index	The RADIUS server index.
server_ip	The IP address of the RADIUS server.

ipv6addr	The IPv6 address of the RADIUS server.
key	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.
default	Sets the **auth_port** to be 1812 and **acct_port** to be 1813.
auth_port	Specifies the UDP port number which is used to transmit RADIUS authentication data between the switch and the RADIUS server.The range is 1 to 65535.
acct_port	Specifies the UDP port number which is used to transmit RADIUS accounting statistics between the switch and the RADIUS server. The range is 1 to 65535.
timeout <int 1-255>	The time in second for waiting server reply. The default value is 5 seconds.
retransmit <int 1-255>	The count for re-transmit. The default value is 2.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a new RADIUS server:

```
DGS-3200-10:4#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-3200-10:4#
```

41-18 config radius delete

Purpose

To delete a RADIUS server.

Format

config radius delete <server_index 1-3>

Description

This command is used to delete a RADIUS server.

Parameters

Parameters	Description
server_index	The RADIUS server index. The range is from 1 to 3.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a RADIUS server:

```
DGS-3200-10:4#config radius delete 1
Command: config radius delete 1


Success.


DGS-3200-10:4#
```

41-19 config radius

Purpose

To configure a RADIUS server.

Format

config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] |key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>| timeout <int 1-255> | retransmit <int 1-255>}

Description

This command is used to configure a RADIUS server.

Parameters

Parameters	Description
server_index	The RADIUS server index.
server_ip	The IP address of the RADIUS server.
ipv6addr	The IPv6 address.
key	The IPv6 address of the RADIUS server.
passwd	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	Specifies the UDP port number which is used to transmit RADIUS authentication data between the switch and the RADIUS server.

acct_port	Specifies the UDP port number which is used to transmit RADIUS accounting statistics between the switch and the RADIUS server.
timeout <int 1-255>	The time in second for waiting server reply. The default value is 5 seconds.
retransmit <int 1-255>	The count for re-transmit. The default value is 2.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a RADIUS server:

```
DGS-3200-10:4#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-3200-10:4#
```

41-20 show radius

Purpose

To display RADIUS server configurations.

Format

show radius

Description

This command is used to display a RADIUS server configurations.

Parameters

None.

Restrictions

None.

Examples

To display RADIUS server configurations:

```
DGS-3200-10:4# show radius
Command: show radius


Index 1
   IP Address     : fe80:fec0:56ab:34b0:20b2:6aff:fecf:7ec6
   Auth—Port     : 1812
   Acct—Port     : 1813
   Timeout        : 5
   Retransmit     : 2
   Key            : adfdslkfjefiefdkgjdassdwtgjk6y1w


Index 2
   IP Address     : 172.18.211.71
   Auth—Port     : 1812
   Acct—Port     : 1813
   Timeout        : 5
   Retransmit     : 2
   Key            : 1234567


Index 3
   IP Address     : 172.18.211.108
   Auth—Port     : 1812
   Acct—Port     : 1813
   Timeout        : 5
   Retransmit     : 2
   Key            : adfdslkfjefiefdkgjdassdwtgjk6y1w



DGS-3200-10:4#
```

41-21 show auth_statistics

Purpose

To display authenticator statistics information

Format

show auth_statistics {ports [<portlist>|all]}

Description

This command is used to display authenticator statistics information

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured.
all	All ports.

Restrictions

None.

Examples

To display authenticator statistics information from port 1:

```
DGS-3200-10:4#show auth_statistics ports 1
Command: show auth_statistics ports 1

Port number : 1

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

DGS-3200-10:4#
```

41-22 show auth_diagnostics

Purpose

To display authenticator diagnostics information

Format

show auth_ diagnostics {ports [<portlist>|all]}

Description

This command is used to display authenticator diagnostics information.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured.
all	All ports.

Restrictions

None.

Examples

To display authenticator diagnostics information from port 1:

```
DGS-3200-10:4# show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

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

DGS-3200-10:4#
```

41-23 show auth_session_statistics

Purpose

To display authenticator session statistics information.

Format

show auth_session_statistics {ports [<portlist>|all]}

Description

This command is used to display authenticator session statistics information.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be configured.
all	All ports.

Restrictions

None.

Examples

To display authenticator session statistics information from port 1:

```
DGS-3200-10:4#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port number : 1

SessionOctetsRx                   0
SessionOctetsTx                   0
SessionFramesRx                   0
SessionFramesTx                   0
SessionId
SessionAuthenticMethod            Remote Authentication Server
SessionTime                       0
SessionTerminateCause             SupplicantLogoff
SessionUserName

DGS-3200-10:4#
```

41-24 show auth_client

Purpose

To display authentication client information.

Format

show auth_client

Description

This command is used to display authentication client information.

Parameters

None.

Restrictions

None

Examples

To display authentication client information:

```
DGS-3200-10:4# 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-3200-10:4#
```

41-25 show acct_client

Purpose

To display account client information.

Format

show acct_client

Description

This command is used to display account client information

Parameters

None.

Restrictions

None.

Examples

To display account client information:

```
DGS-3200-10:4# 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-3200-10:4#
```

42 Access Authentication Control Command List

```
enable authen_policy
disable authen_policy
show authen_policy
create authen_login method_list_name <string 15>
config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name <string 15>
show authen_login [default | method_list_name <string 15> | all]
create authen_enable method_list_name <string 15>
config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}
delete authen_enable method_list_name <string 15>
show authen_enable [default | method_list_name <string 15> | all]
config authen application [console | telnet | ssh | http |all] [login | enable] [default| method_list_name <string 15>]
show authen application
create authen server_group <string 15>
config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> 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 1-255> }
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 1-255> }
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 <password 0-15>
```

42-1 enable authen_policy

Purpose

To enable system access authentication policy.

Format

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.

Parameters

None

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable system access authentication policy:

```
DGS-3200-10:4#enable authen_policy
Command: enable authen_policy

Success.

DGS-3200-10:4#
```

42-2 disable authen_policy

Purpose

To disable system access authentication policy.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable system access authentication policy:

```
DGS-3200-10:4#disable authen_policy
Command: disable authen_policy


Success.


DGS-3200-10:4#
```

42-3 show authen_policy

Purpose

To display whether system access authentication policy is enabled or disabled.

Format

disable authen_policy

Description

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

Parameters

None.

Restrictions

None.

Examples

To display system access authentication policy:

```
DGS-3200-10:4#show authen_policy
Command: show authen_policy


Authentication Policy : Enabled


DGS-3200-10:4#
```

42-4 create authen_login method_list_name

Purpose

To create a user-defined method list of authentication methods for user login.

Format

create authen_login method_list_name <string 15>

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.

Parameters

Parameters	Description
string 15	The user-defined method list name.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4#create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1


Success.


DGS-3200-10:4#
```

42-5 config authen_login

Purpose

To configure a user-defined or default method list of authentication methods for user login.

Format

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

Description

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

Parameters

Parameters	Description
default	The default method list of authentication methods.
method_list_name <string 15>	The user-defined method list of authentication methods.
tacacs	Authentication by the built-in server group **tacacs**.
xtacacs	Authentication by the built-in server group **xtacacs**.
tacacs+	Authentication by the built-in server group **tacacs+**.
radius	Authentication by the built-in server group **radius**.
server_group <string 15>	Authentication by the user-defined server group.
local	Authentication by local user accout database in device.
none	No authentication.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4#config authen_login method_list_name login_list_1 method tacacs+
tac
acs local
Command: config authen_login method_list_name login_list_1 method tacacs+ tacac
s local

Success.

DGS-3200-10:4#
```

42-6 delete authen_login method_list_name

Purpose

To delete a user-defined method list of authentication methods for user login.

Format

delete authen_login method_list_name <string 15>

Description

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

Parameters

Parameters	Description
string 15	The user-defined method list name.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4#delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1


Success.


DGS-3200-10:4#
```

42-7 show authen_login

Purpose

To display the method list of authentication methods for user login.

Format

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

Description

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

Parameters

Parameters	Description
default	Display default user-defined method list for user login.
method_list_name <string 15>	Display the specific user-defined method list for user login.
all	Display all method lists for user login.

Restrictions

None.

Examples

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

```
DGS-3200-10:4#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-3200-10:4#
```

42-8 create authen_enable method_list_name

Purpose

To create a user-defined method list of authentication methods for promoting a user's privilege to Administrator level.

Format

create authen_enable method_list_name <string 15>

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.

Parameters

Parameters	Description
string 15	The user-defined method list name.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4#create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1


Success.


DGS-3200-10:4#
```

42-9 config authen_enable

Purpose

To configure a user-defined or default method list of authentication methods for promoting a user's privilege to Administrator level.

Format

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

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 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 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_password".

Parameters

Parameters	Description
default	The default method list of authentication methods.
method_list_name <string 15>	The user-defined method list of authentication methods.

tacacs	Authentication by the built-in server group **tacacs**.
xtacacs	Authentication by the built-in server group **xtacacs**.
tacacs+	Authentication by the built-in server group **tacacs+**.
radius	Authentication by the built-in server group **radius**.
server_group <string 15>	Authentication by the user-defined server group.
local_enable	Authentication by local enable password in device.
none	No authentication.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
 DGS-3200-10:4#config authen_enable method_list_name enable_list_1 method tacacs+
tac
 acs local_enable
 Command: config authen_ enable method_list_name enable_list_1 method tacacs+ tacac
 s local_enable

 Success.

 DGS-3200-10:4#
```

42-10 delete authen_enable method_list_name

Purpose

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>

Description

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

Parameters

Parameters	Description
string 15	The user-defined method list name

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4#delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1


Success.


DGS-3200-10:4#
```

42-11 show authen_enable

Purpose

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]

Description

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

Parameters

Parameters	Description
default	Display default user-defined method list for promoting a user's privilege to Administrator level.
method_list_name <string 15>	Display the specific user-defined method list for a promoting user's privilege to Administrator level.
all	Display all method lists for promoting a user's privilege to Administrator level.

Restrictions

None.

Examples

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

```
DGS-3200-10:4#show authen_enable all
Command: show authen_enable all

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

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

Total Entries : 2

DGS-3200-10:4#
```

42-12 config authen application

Purpose

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>]

Description

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

Parameters

Parameters	Description
console	Application: console.
telnet	An application: Telnet.
ssh	An application: SSH.
http	An application: web.
all	Applications: **console**, **telnet**, **SSH**, and **web**.
login	Select the method list of authentication methods for user login.
enable	Select the method list of authentication methods for promoting user's privilege to Admin level.

default	The default method list.
method_list_name **<string 15>**	The user-defined method list name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the login method list for Telnet:

```
 DGS-3200-10:4#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-3200-10:4#
```

42-13 show authen application

Purpose

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

Format

show authen application

Description

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

Parameters

None.

Restrictions

None.

Examples

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

```
DGS-3200-10:4#show authen application
Command: show authen application


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


DGS-3200-10:4#
```

42-14 create authen server_group

Purpose

To create a user-defined authentication server group.

Format

create authen server_group <string 15>

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.

Parameters

Parameters	Description
string 15	The user-defined server group name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a user-defined authentication server group:

```
DGS-3200-10:4#create authen server_group mix_1
Command: create authen server_group mix_1


Success.


DGS-3200-10:4#
```

42-15 config authen server_group

Purpose

To add or remove an authentication server host to or from the specified server group.

Format

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

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**.

Parameters

Parameters	Description
server_group tacacs	The built-in server group **tacacs**.
server_group xtacacs	The built-in server group **xtacacs**.
server_group tacacs+	The built-in server group **tacacs+**.
server_group radius	The built-in server group **radius**.
server_group <string 15>	A user-defined server group.
add	Add a server host to a server group.
delete	Remove a server host from a server group.
server_host <ipaddr>	The server host's IP address.
protocol tacacs	The server host's authentication protocol.
protocol xtacacs	The server host's authentication protocol.
protocol tacacs+	The server host's authentication protocol.
protocol radius	The server host's authentication protocol.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add an authentication server host to a server group:

```
DGS-3200-10:4#config authen server_group mix_1 add server_host 10.1.1.222 protocol
tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol ta
cacs+

Success.

DGS-3200-10:4#
```

42-16 delete authen server_group

Purpose

To delete a user-defined authentication server group.

Format

delete authen server_group <string 15>

Description

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

Parameters

Parameters	Description
string 15	The user-defined server group name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a user-defined authentication server group:

```
DGS-3200-10:4#delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DGS-3200-10:4#
```

42-17 show authen server_group

Purpose

To display the authentication server groups.

Format

show authen server_group {<string 15>}

Description

This command is used to display the authentication server groups.

Parameters

Parameters	Description
<string 15>	The built-in or user-defined server group name.

Restrictions

None.

Examples

To display all authentication server groups:

```
DGS-3200-10:4#show authen server_group
Command: show authen server_group

Server Group : mix_1

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-3200-10:4#
```

42-18 create authen server_host

Purpose

To create an authentication server host.

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 1-255> }

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.

Parameters

Parameters	Description	
server_host <ipaddr>	The server host's IP address.	
protocol tacacs	The server host's authentication protocol.	
protocol xtacacs	The server host's authentication protocol.	
protocol tacacs+	The server host's authentication protocol.	
protocol radius	The server host's authentication protocol.	
port <int 1-65535>	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.	
key	**<key_string 254>**	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 <int 1-255>	The time in seconds for waiting for a server reply. Default value is 5 seconds.	
retransmit <int 1-255>	The count for re-transmit. This value is meaningless for TACACS+. Default value is 2.	

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4#create authen server_host 10.1.1.222 protocol tacacs+ port 15555 time
out 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555 timeou
t 10

Success.

DGS-3200-10:4#
```

42-19 config authen server_host

Purpose

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 1-255> }

Description

This command is used to configure an authentication server host.

Parameters

Parameters	Description	
server_host <ipaddr>	The server host's IP address.	
protocol tacacs	The server host's authentication protocol.	
protocol xtacacs	The server host's authentication protocol.	
protocol tacacs+	The server host's authentication protocol.	
protocol radius	The server host's authentication protocol.	
port <int 1-65535>	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.	
key	**<key_string 254>**	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 <int 1-255>	The time in seconds for waiting for a server reply. The default value is 5 seconds.	

retransmit <int 1-255>	The count for re-transmit. This value is meaningless for TACACS+. The default value is 2.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
 DGS-3200-10:4#config authen server_host 10.1.1.222 protocol tacacs+ key "This is
a secret"
 Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a se
 cret"

 Success.

 DGS-3200-10:4#
```

42-20 delete authen server_host

Purpose

To delete an authentication server host.

Format

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

Description

This command is used to delete an authentication server host.

Parameters

Parameters	Description
server_host <ipaddr>	The server host’s IP address.
protocol tacacs	The server host’s authentication protocol.
protocol xtacacs	The server host’s authentication protocol.
protocol tacacs+	The server host’s authentication protocol.
protocol radius	The server host’s authentication protocol.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an authentication server host:

```
DGS-3200-10:4#delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

DGS-3200-10:4#
```

42-21 show authen server_host

Purpose

To display the authentication server hosts.

Format

show authen server_host

Description

This command is used to display authentication server hosts.

Parameters

None

Restrictions

None

Examples

To display all authentication server hosts:

```
DGS-3200-10:4#show authen server_host
Command: show authen server_host

SRV IP Address   Protocol  Port   Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  -------------------------
10.1.1.222       TACACS+   15555  10       No Use      This is a secret

Total Entries : 1

DGS-3200-10:4#
```

42-22 config authen parameter response_timeout

Purpose

To configure the amount of time waiting or for user input on console, Telnet, and SSH applications.

Format

config authen parameter response_timeout <int 0-255>

Description

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

Parameters

Parameters	Description
<int 0-255>	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.

Examples

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

```
DGS-3200-10:4#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60


Success.


DGS-3200-10:4#
```

42-23 config authen parameter attempt

Purpose

To configure the maximum attempts for users trying to login or promote the privilege on console, Telnet, or SSH applications.

Format

config authen parameter attempt <int 1-255>

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.

Parameters

Parameters	Description
<int 1-255>	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.

Examples

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

```
DGS-3200-10:4#config authen parameter attempt 9
Command: config authen parameter attempt 9


Success.


DGS-3200-10:4#
```

42-24 show authen parameter

Purpose

To display the parameters of authentication.

Format

show authen parameter

Description

This command is used to display the authentication parameters.

Parameters

None.

Restrictions

None.

Examples

To display the authentication parameters:

```
DGS-3200-10:4# show authen parameter
Command: show authen parameter

Response timeout : 60 seconds
User attempts    : 9

DGS-3200-10:4#
```

42-25 enable admin

Purpose

To open the administrator level privilege

Format

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 can not be used when authentication policy is disabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable administrator lever privilege:

```
DGS-3200-10:3#enable admin
Password:********

DGS-3200-10:4#
```

42-26 config admin local_enable

Purpose

To configure the local enable password for the administrator level privilege.

Format

config admin local_enable <password 0-15>

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.

Parameters

Parameters	Description
password 0-15	The specific password.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the administrator password:

```
DGS-3200-10:4#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-3200-10:4#
```

43 SSL Command List

show ssl certificate
download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
enable ssl { ciphersuite { RSA_with_RC4_128_MD5 | **RSA_with_3DES_EDE_CBC_SHA |** **DHE_DSS_with_3DES_EDE_CBC_SHA |** **RSA_EXPORT_with_RC4_40_MD5 } }**
disable ssl { ciphersuite { RSA_with_RC4_128_MD5 | **RSA_with_3DES_EDE_CBC_SHA |** **DHE_DSS_with_3DES_EDE_CBC_SHA |** **RSA_EXPORT_with_RC4_40_MD5 } }**
show ssl
show ssl cachetimout
config ssl cachetimout <value 60-86400>

43-1 show ssl certificate

Purpose

To show the certificate status.

Format

show ssl certificate

Description

This command is used to download specified certificate types according to the desired key exchange algorithm. The options are no certificate, RSA type or DSA type certificate

Parameters

None.

Restrictions

None.

Examples

To show certificate:

```
DGS-3200-10:4#show ssl certificate
Command: show ssl certificate


Loaded with RSA Certificate!


DGS-3200-10:4#
```

43-2 download ssl certificate

Purpose

To download certificate to device according to certificate level.

Format

download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

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.

Parameters

Parameters	Description
ipaddr	Input the TFTP server IP address.
certfilename	The desired certificate file name.
path_filename	Certificate file path in respect to the TFTP server root path. Input characters with a maximum of 64 octets.
keyfilename	The private key file name which accompanies the certificate.
path_filename	Private key file path in respect to the TFTP server root path. Input characters with a maximum of 64 octets.

Restrictions

Only Administrator-level users can issue this command.

Examples

To download a certificate from a TFTP server:

```
 DGS-3200-10:4# 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-3200-10:4#
```

43-3 enable ssl

Purpose

To enable the SSL feature and ciphersuites.

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 } }

Description

This command is used to enable the SSL status and its individual ciphersuites. Using the **enable ssl** command will enable the SSL feature, which means SSLv3 and TLSv1. Each ciphersuite must be enabled by this command.

Parameters

Parameters	Description
ciphersuite	For configuring a cipher suite combination.
RSA_with_RC4_128_MD5	Indicates RSA key exchange with RC4 128 bits encryption and MD5 hash.
RSA_with_3DES_EDE_CBC_SHA	Indicates RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
DHE_DSS_with_3DES_EDE_CBC_SHA	Indicates DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
RSA_EXPORT_with_RC4_40_MD5	Indicates RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.
NULL	Enable the SSL feature.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3200-10:4# enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3200-10:4#
```

To enable SSL:

```
DGS-3200-10:4# enable ssl
Command: enable ssl

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

DGS-3200-10:4#
```

43-4 disable ssl

Purpose

To disable SSL feature and 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 } }

Description

This command is used to disable the SSL feature and supported ciphersuites.

Parameters

Parameters	Description
ciphersuite	For configuring cipher suite combination.
RSA_with_RC4_128_MD5	Indicates RSA key exchange with RC4 128 bits encryption and MD5 hash.
RSA_with_3DES_EDE_CBC_SHA	Indicates RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.

DHE_DSS_with_3DES_EDE_CBC_SHA	Indicates DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
RSA_EXPORT_with_RC4_40_MD5	Indicates RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.
NULL	Disables the SSL feature.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3200-10:4# disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3200-10:4#
```

To disable the SSL feature:

```
DGS-3200-10:4# disable ssl
Command: disable ssl

Success.

DGS-3200-10:4#
```

43-5 show ssl

Purpose

To display SSL environment variables and ciphersuites status.

Format

show ssl

Description

This command is used to display the current SSL status and supported ciphersuites.

Parameters

None.

Restrictions

None.

Examples

To display SSL:

```
DGS-3200-10:4# show ssl
Commands: show ssl

SSL Status                                              Disabled
RSA_WITH_RC4_128_MD5                       0x0004   Enabled
RSA_WITH_3DES_EDE_CBC_SHA                  0x000A   Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA              0x0013   Enabled
RSA_EXPORT_WITH_RC4_40_MD5                 0x0003   Enabled

DGS-3200-10:4#
```

43-6 show ssl cachetimeout

Purpose

To display the SSL cache timeout value.

Format

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.

Parameters

None.

Restrictions

None.

Examples

To show the SSL cache timeout:

```
DGS-3200-10:4# show ssl cachetimeout
Commands: show ssl cachetimeout


Cache timeout is 600 second(s)


DGS-3200-10:4#
```

43-7 config ssl cachetimeout

Purpose

To configure the SSL cache timeout value. This value is between 1 minute and 24 hours.

Format

config ssl cachetimout <value 60-86400>

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 theweb 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.

Parameters

Parameters	Description
cachetimout	The SSL cache timeout value attributes.

Restrictions

None.

Examples

To configure an SSL cache timeout value of 60:

```
DGS-3200-10:4# config ssl cachetimeout 60
Commands: config ssl cachetimeout 60


Success.
DGS-3200-10:4#
```

44 SSH Command List

config ssh algorithm [3DES| AES128| AES192| AES256| arcfour|blowfish| cast128| twofish128| twofish192| twofish256| MD5| SHA1| RSA| DSA] [enable| disable]
show ssh algorithm
config ssh authmode [password|publickey|hostbased] [enable|disable]
show ssh authmode
config ssh user <username 15> authmode [publickey | password | hostbased [hostname <domain_name 32> |hostname_IP <domain_name 32> <ipaddr>]]
show ssh user authmode
config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min |30min |60min |never] }
enable ssh
disable ssh
show ssh server

44-1 config ssh algorithm

Purpose

To configure the SSH server algorithm.

Format

config ssh algorithm [3DES|AES128|AES192|AES256|arcfour|blowfish|cast128|twofish128| twofish192|twofish256|MD5|SHA1|RSA|DSS] [enable|disable]

Description

This command is used to configure the SSH service algorithm.

Parameters

Parameters	Description
3DES	An SSH server encryption algorithm.
blowfish	An SSH server encryption algorithm.
AES(128,192,256)	An SSH server encryption algorithm.
arcfour	An SSH server encryption algorithm.
cast128	An SSH server encryption algorithm.
twofish(128,192,256)	An SSH server encryption algorithm.
MD5	An SSH server data integrality algorithm.
SHA1	An SSH server data integrality algorithm.

DSS	An SSH server public key algorithm.
RSA	An SSH server public key algorithm.
enable	Used to enable the algorithm.
disable	Used to disable the alogirthm.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable an SSH server public key algorithm:

```
DGS-3200-10:4#config ssh algorithm DSA enable RSA enable
Command: config ssh algorithm DSA enable RSA enable


Success.


DGS-3200-10:4#
```

44-2 show ssh algorithm

Purpose

To show the SSH server algorithms.

Format

show ssh algorithm

Description

This command is used to display the SSH service algorithms.

Parameters

None.

Restrictions

None.

Examples

To show the SSH server algorithms:

```
DGS-3200-10:4#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-3200-10:4#
```

44-3 config ssh authmode

Purpose

To update user authentication for SSH configuration.

Format

config ssh authmode [password|publickey|hostbased][enable|disable]

Description

This command is used to update the SSH user information.

Parameters

Parameters	Description
password	Specifies user authentication method.
publickey	Specifies user authentication method.
hostbased	Specifies user authentication method.
enable	Enable user authentication method.
disable	Disable user authentication method.

Restrictions

Only Administrator-level users can issue this command.

Examples

To config the SSH user authentication method:

```
DGS-3200-10:4#config ssh authmode publickey enable
Command: config ssh authmode publickey enable


Success.


DGS-3200-10:4#
```

44-4 show ssh authmode

Purpose

To display user authentication method

Format

show ssh authmode

Description

This command is used to display the user authentication method.

Parameters

None.

Restrictions

None.

Examples

To display the SSH user authentication method:

```
DGS-3200-10:4#show ssh authmode
Command: show ssh authmode


The SSH Authmode
-------------------------------------------------------
Password  : Enabled
Publickey : Enabled
Hostbased : Enabled


DGS-3200-10:4#
```

44-5 config ssh user

Purpose

To update user information for SSH configuration.

Format

config ssh user <username 15> authmode [publickey | password | hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>]]

Description

This command is used to update SSH user information

Parameters

Parameters	Description
username 15	The user name.
publickey	Specifies user authentication method.
password	Specifies user authentication method.
hostbased	Specifies user authentication method.
hostname	Specifies host domain name.
hostname_IP	Specifies host domain name and IP address.
domain_name	Specifies host name if configuration is in host-based mode.
ipaddr	Specifies host IP address if configuring host-based mode.

Restrictions

Only Administrator-level users can issue this command.

Note: The user account must be created.

Examples

To update user “danilo” authmode:

```
DGS-3200-10:4#config ssh user danilo publickey
Command: config ssh user danilo publickey

Success.

DGS-3200-10:4#
```

44-6 show ssh user authmode

Purpose

To show SSH user information.

Format

show ssh user authmode

Description

This command is used to display SSH user information.

Parameters

None.

Restrictions

None.

Examples

To show user information about SSH configuration:

```
DGS-3200-10:4#show ssh user
Command: show ssh user

Current Accounts
Username       Authentication
-------------  -------------
danilo         publickey

Total Entries : 1

DGS-3200-10:4#
```

44-7 config ssh server

Purpose

To configure the SSH server.

Format

config ssh server {maxsession <int 1-8>| contimeout <sec 120-600> | authfail {<int 2-20> | rekey [10min|30min|60min|never] }

Description

This command is used to configure SSH server general information.

Parameters

Parameters	Description
int 1-8	Specifies SSH server max session at the same time.
sec 120-600	Specifies SSH server connection timeout.
int 2-20	Specifies user max fail attempts.
10/30/60 min	Specifies time to re-generate session key.
never	Do not re-generate session key.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure an SSH server max session of 3:

```
DGS-3200-10:4#config ssh server maxsession 3
Command: config ssh server maxsession 3


Success.


DGS-3200-10:4#
```

44-8 enable ssh

Purpose

To enable the SSH server.

Format

enable ssh server

Description

This command is used to enable SSH server services.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command. When enabling SSH, Telnet is disabled.

Examples

To enable SSH:

```
DGS-3200-10:4#enable ssh
Command: enable ssh


Success.


DGS-3200-10:4#
```

44-9 disable ssh

Purpose

To disable SSH server service.

Format

disable ssh server

Description

This command is used to disable SSH server services.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable SSH:

```
DGS-3200-10:4#disable ssh
Command: disable ssh


Success.


DGS-3200-10:4#
```

44-10 show ssh server

Purpose

To show SSH server information.

Format

show ssh server

Description

This command is used to display SSH server general information.

Parameters

None.

Restrictions

None.

Examples

To show SSH server:

```
DGS-3200-10:4#show ssh server
Command: show ssh server


The SSH Server Configuration
max Session          : 3
Connection Timeout : 300
Authfail Attempts   : 2
Rekey Timeout        : 60min


DGS-3200-10:4#
```

45 IP-MAC-Port Binding (IMPB) Command List

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports[<portlist>| all]}

config address_binding ip_mac ports[<portlist> | all] {state [enable {[strict | loose]} | disable] |allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | mode [arp | acl]}

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist>| all]}

delete address_binding [ip_mac[ipaddress<ipaddr> [mac_address <macaddr>] |all] |blocked[all | vlan_name<vlan_name> mac_address <macaddr>]]

show address_binding [ip_mac [all| ipaddress <ipaddr> mac_address <macaddr>]|blocked [all| vlan_name <vlan_name> mac_address <macaddr>] |ports]

enable address_binding trap_log

disable address_binding trap_log

enable address_binding dhcp_snoop

disable address_binding dhcp_snoop

clear address_binding dhcp_snoop binding_entry ports [<portlist>|all]

show address_binding dhcp_snoop {[max_entry { ports <portlist>} | binding_entry {port <port>}]}

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit]

45-1 create address_binding ip_mac ipaddress

Purpose

To create an IP-MAC Binding entry.

Format

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports[<portlist>| all] }

Description

This command is used to create an IP-MAC Binding entry.

Parameters

Parameters	Description
ipaddr	The IP address.
macaddr	The MAC address.
ports	Configure the portlist to apply, if not configure ports means apply to all ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create address binding on the Switch:

```
 DGS-3200-10:4#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-3200-10:4#
```

45-2 config address_binding ip_mac ports

Purpose

To configure an IP-MAC state to enable or disable for specified ports.

Format

config address_binding ip_mac ports[<portlist> | all] {state [enable {[strict | loose]} | disable] |allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | mode [arp | acl] }

Description

This command is used to configure the per port state of IP-MAC binding in the switch.
If a port has been configured as group member of an aggregagted link, then it can not enable its IP-MAC 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 ACL mode or ARP mode. In ARP mode, only ARP packets are checked for binding. In ACL mode, both ARP packets and IP packets are checked for the binding. Therefore, ACL mode provides more strict checks for packets.

When configuring the port mode to ACL , the switch will create ACL access entries corresponding to the entries of this port. If the port changes to ARP, all the ACL access entries will be deleted automatically.

Parameters

Parameters	Description
state	Configure the address binding port state to **enable** or **disable**.

	When this is enabled, the port will perform the binding check.
strict	This mode provides a stricter method of control. If a user chooses it, all packets will be sent to the CPU, which means all packets will not be forwarded by the hardware until the software learns entries for the port. The port will check ARP packets and IP packets by IP-MAC-port binding entries. If the packet is found by the entry, the MAC will be set to dynamic. If the packet isn't found by the entry, the MAC will be set to block. Other packets will be dropped. The default mode is **strict** if not specified.
loose	This mode provides a more loose method of control. If user chooses it, ARP packets and IP Broadcast packets will go to the CPU. The packets will still be forwarded by the hardware until a specific source MAC is blocked by the software. The port will check ARP packets and IP Broadcast packets by IP-MAC-port binding entries. If the packet is found by the entry, the MAC will be set to dynamic. If the packet isn't found by the entry, the MAC will be set to block. Other packets will be bypassed.
allow_zeroip	Specify whether to allow ARP packets with SIP address 0.0.0.0.. 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. When set to disable, this option does not affect the IP-MAC-port binding ACL Mode.
forward_dhcppkt	By default, the DHCP packets with broadcast DA will be flooded.When set to disabled, the broadcast DHCP packets received by the specified port will not be forwarded. 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.
mode	When configuring the port to ACL mode, the switch will create ACL access entries corresponding to the entries of this port. If the port changes to ARP, all the ACL access entries will be deleted automatically. The default mode of port is ARP mode.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure port 1 to be enabled for address binding:

```
 DGS-3200-10:4# config address_binding ip_mac ports 1 state
enable
 Command: config address_binding ip_mac ports 1 state enable

 Success.

 DGS-3200-10:4#
```

```
 DGS-3200-10:4# config address_binding ip_mac ports 1 state
enable
 Command: config address_binding ip_mac ports 1 state enable

 Success.

 DGS-3200-10:4# show access_profile
 Command: show access_profile
 Access Profile Table

 Access Profile ID : 1
 Type      : Packet Content Filter
 Owner     : Address_binding
 Masks     :
 Offset 0-15  : 0x00000000 0000ffff ffffffff 00000000
 Offset 16-31 : 0x00000000 00000000 00000000 0000ffff
 Offset 32-47 : 0xffff0000 00000000 00000000 00000000
 Offset 48-63 : 0x00000000 00000000 00000000 00000000
 Offset 64-79 : 0x00000000 00000000 00000000 00000000

 Access Profile ID : 2
 Type      : Packet Content Filter
 Owner     : Address_binding
 Masks     :
 Offset 0-15  : 0x00000000 00000000 00000000 00000000
 Offset 16-31 : 0xffff0000 00000000 00000000 00000000
 Offset 32-47 : 0x00000000 00000000 00000000 00000000
 Offset 48-63 : 0x00000000 00000000 00000000 00000000
 Offset 64-79 : 0x00000000 00000000 00000000 00000000


 Access ID: 1
 Mode     : Deny
 Owner    : Address_binding
 Port     : 1
 ----------------------------------------------------
 Offset 0-15  : 0x00000000 00000000 00000000 00000000
 Offset 16-31 : 0x08000000 00000000 00000000 00000000
 Offset 32-47 : 0x00000000 00000000 00000000 00000000
 Offset 48-63 : 0x00000000 00000000 00000000 00000000
 Offset 64-79 : 0x00000000 00000000 00000000 00000000
```

45-3 config address_binding address

Purpose

To update an address binding entry.

Format

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> { ports [portlist | all] }

Description

This command is used to update an address binding entry.

Parameters

Parameters	Description
ipaddr	The IP address.
macaddr	The MAC address.
ports	Configure the portlist to apply, if ports are not configured, then it will apply to all ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure an address binding entry :

```
 DGS-3200-10:4#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-3200-10:4#
```

45-4 delete address_binding address

Purpose

To delete an address binding entry.

Format

delete address_binding [ip-mac [ipaddress <ipaddr> [mac_address <macaddr>] |all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]

Description

This command is used to delete an address binding entry. If ACL mode is enabled, the switch will delete the according ACL access entries automatically.

Parameters

Parameters	Description
ip_mac	The database that a user creates for address binding.
blocked	The address database that the system auto learned and blocked.
ipaddr	The IP address.
macaddr	The MAC address.
vlan_name	The VLAN name (the blocked MAC belongs to).

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an address binding entry:

```
 DGS-3200-10:4#delete 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-3200-10:4#
```

45-5 show address_binding

Purpose

To display address binding entries, blocked MAC entries, and port status.

Format

show address_binding [ip_mac [all| ipaddress <ipaddr> mac_address <macaddr>] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>] | ports]

Description

This command is used to display address binding information.

Parameters

Parameters	Description
ip_mac	The database that user create for address binding.
blocked	The address database that system auto learned and blocked.
ipaddr	The IP address.
macaddr	The MAC address.
vlan_name	The VLAN name (the blocked MAC belongs to).
ports	The state of IP MAC port binding of all the ports.

.

Restrictions

None.

Examples

To display the address binding global configuration:

```
DGS-3200-10:4#show address_binding ip_mac
Command: show address_binding ip_mac


ACL_mode : Disabled
Trap/Log : Disabled
Enabled Ports:
Enabled Allow Zero IP Ports:
IP Address      MAC Address        Mode  Ports
--------------- -----------------  ----  ------------------------------


10.90.90.1      00-11-22-33-44-55  ARP   2
10.90.90.2      00-11-22-33-44-55  ARP   1-9


Total Entries : 2DGS-3200-10:4#
```

45-6 enable address_binding trap_log

Purpose

To enable an address binding trap/log.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable an address binding trap log:

```
DGS-3200-10:4#enable address_binding trap_log
Command: enable address_binding trap_log


Success.


DGS-3200-10:4#
```

45-7 disable address_binding trap_log

Purpose

To disable the address binding trap/log.

Format

disable address_binding trap_log.

Description

This command is used to disable address binding trap logs.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the address binding trap log:

```
DGS-3200-10:4#disable address_binding trap_log
Command: disable address_binding trap_log


Success.


DGS-3200-10:4#
```

45-8 enable address_binding dhcp_snoop

Purpose

To enable the address binding auto mode.

Format

enable address_binding dhcp_snoop

Description

This command is used to enable the address binding 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 allow zero ip function is disabled on this port.

The auto-learned IP-MAC binding entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an ACL-mode 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 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 mode, 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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the address binding auto mode:

```
DGS-3200-10:4#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop


Success.


DGS-3200-10:4#
```

45-9 disable address_binding dhcp_snoop

Purpose

To disable the address binding ACL mode.

Format

disable address_binding dhcp_snoop

Description

When this is disabled, all of the auto-learned binding entries will be removed.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the address binding auto mode:

```
DGS-3200-10:4#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop


Success.


DGS-3200-10:4#
```

45-10 clear address_binding dhcp_snoop

Purpose

To clear the address binding entries learned for the specified ports.

Format

clear address_binding dhcp_snoop binding_entry ports [<portlist>|all]

Description

This command is used to clear the address binding entries learned for the specified ports.

Parameters

Parameters	Description
ports	Specifies the list of ports that you would like to clear the DHCP-snoop learned entry.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear the address binding entries for ports 1 to 3:

```
DGS-3200-10:4# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3


Success.


DGS-3200-10:4#
```

45-11 show address_binding dhcp_snoop

Purpose

To show the address binding auto learning databases.

Format

show address_binding dhcp_snoop {[max_entry { ports <portlist>} | binding_entry {port <port>}]}

Description

This command is used to display all the auto-learning databases.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display address binding DHCP snooping:

```
 DGS-3200-10:#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop
 DHCP_Snoop : Enabled


 DGS-3200-10:4#
```

To display the DHCP Snooping binding entry:

```
DGS-3200-10:#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry
IP Address        MAC Address        Lease Time(secs)   Port      Status
---------------   -----------------   ----------------  --------  ---------
10.62.58.35       00-0B-5D-05-34-0B  35964              1          Active
10.33.53.82       00-20-c3-56-b2-ef  2590               2          Inactive

Total entries : 2
DGS-3200-10:4#
```

Note: “Inactive” indicates that the entry is currently inactive due to port link down.

```
 DGS-3200-10:#show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry
 Port  Max Entry
 ----  ---------
 1      10
 2      10
 3      10
 4      no_limit
 5      no limit
 6      no_limit
 7      no limit
 8      no_limit
 9      no_limit
 10     no_limit

 DGS-3200-10:4#
```

45-12 config address_binding dhcp_snoop max_entry

Purpose

To specify the maximum number of entries which can be learned by the specified ports.

Format

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit]

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.

Parameters

Parameters	Description
portlist	Specifies the list of ports that you would like to clear the DHCP-snooping learned entry.
limit	Specifies the maxium number.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the maximum number of entries that ports 1 to 3 can learn to 10:

```
DGS-3200-10:4# 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-3200-10:4#
```

46 Web-based Access Control Command List

enable wac

disable wac

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>] }

config wac method [local | radius]

config wac auth_failover [enable | disable]

config wac default_redirpath <string 128>

config wac clear_default_redirpath

config wac virtual_ip <ipaddr>

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> } {authenticated | authenticating | blocked}

clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr> }]

46-1 enable wac

Purpose

To enable the Web-based Access Control function.

Format

enable wac

Description

This command is used to enable the WAC function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the WAC function:

```
DGS-3200-10:4# enable wac
Command: enable wac


Success.


DGS-3200-10:4#
```

46-2 disable wac

Purpose

To disable the Web-based Access Control function.

Format

disable wac

Description

This command is used to disable the WAC function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the WAC function:

```
DGS-3200-10:4# disable wac
Command: disable wac


Success.


DGS-3200-10:4#
```

46-3 config wac ports

Purpose

To configure the WAC port level setting.

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>] }

Description

This command is used to configure the Web authentication setting.

Parameters

Parameters	Description
state	Specifies to enable or disable WAC state.
aging_time	A time period during which an authenticated host will be kept in authenticated state. **infinite** indicates the authenticated host on the port will not ageout. The default value is 24 hours.
idle_time	A time period after which an authenticated host will be moved to un-authenticated state if there is no traffic during that period. **infinite** indicates the host will not be removed from the authenticated state due to idle of traffic. The default value is **infinite**.
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.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the WAC port state:

```
DGS-3200-10:4# config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable


Success.


DGS-3200-10:4#
```

To configure port aging time:

```
DGS-3200-10:4# config wac aging_time 100
Command: config wac aging_time 100


Success.


DGS-3200-10:4#
```

46-4 config wac

Purpose

To configure the Web authentication global parameters.

Format

config wac method [local | radius]

Description

This command is used to configure the global parameters for Web authentication.

Parameters

Parameters	Description
method	Specify the authenticated method
local	The authentication will be done via the local database.
radius	The authentication will be done via the RADIUS server.
mode	The mode can be either port-based or host-based.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the authentication method:

```
DGS-3200-10:4# config wac method radius
Command: config wac method radius


Success.


DGS-3200-10:4#
```

46-5 config wac auth_failover

Purpose

To configure WAC authentication failover.

Format

config wac auth_failover [enable | disable]

Description

This command is used to configure WAC authentication failover. By default, the authentication failover is disabled. If RADIUS servers are unreachable, the authentication will fail. When the authentication failover is enabled, if RADIUS server authentication is unreachable, the local database will be used to do the authentication.

Parameters

Parameters	Description
enable	Enable the protocol authentication failover.
disable	Disable the protocol authentication failover.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure WAC authentication failover:

```
DGS-3200-10:4# config wac auth_failover
Command: config wac auth_failover


Success.


DGS-3200-10
```

46-6 config wac default_redirpath

Purpose

To configure the WAC default redirect path.

Format

config wac default_redirpath <string 128>

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.

Parameters

Parameters	Description
<string 128>	The URL that the client will be redirected to after successful authentication. By default, the redirected path is cleared

Restrictions

Only Administrator-level users can issue this command.

Example

To configure WAC default redirect path:

```
DGS-3200-10:config wac default_redirpath http://www.dlink.com
Command: config wac default_redirpath http://www.dlink.com


Success.


DGS-3200-10:
```

46-7 config wac clear_default_redirpath

Purpose

To clear WAC default redirect path.

Format

config wac clear_default_redirpath

Description

This command is used to clear a WAC default redirect path. When the string is cleared, the client will not be redirected to another URL after successful authentication.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To clear a WAC default redirect path:

```
DGS-3200-10:4# config wac clear_default_redirpath
Success.


DGS-3200-10:4#
```

46-8 config wac virtual_ip

Purpose

To configure the WAC virtual IP address used to accept authentication requests from unauthenticated hosts.

Format

config wac virtual_ip <ipaddr>

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.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the virtual IP.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the WAC virtual IP address used to accept authentication requests from unauthenticated hosts:

```
DGS-3200-10:4# config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1


Success.


DGS-3200-10:4#
```

46-9 config wac switch_http_port

Purpose

To configure the TCP port which the WAC switch listens to.

Format

config wac switch_http_port < tcp_port_number 1-65535> {[http | https]}

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.

Parameters

Parameters	Description
<tcp_port_number 1-65535>	A TCP port which the WAC switch listens to and uses to finish the authenticating process.
http	Specifies that WAC runs HTTP protocol on this TCP port.
https	Specifies that WAC runs HTTPS protocol on this TCP port.

Restrictions

The HTTP cannot run at TCP port 443, and the HTTPS cannot run at TCP port 80. Only Administrator-level users can issue this command.

Example

To configure a TCP port which the WAC switch listens to:

```
DGS-3200-10:4# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DGS-3200-10:4#
```

46-10 create wac user

Purpose

To create user accounts for Web-based Access Control.

Format

create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

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.

Parameters

Parameters	Description
username	User account for Web-based Access Control.
vlan	The authentication VLAN name.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a WAC account:

```
DGS-3200-10:4# create wac user vlan 123
Command: create wac user vlan 123
Enter a case-sensitive new password:**
 Enter the new password again for confirmation:**
Success.

DGS-3200-10:4#
```

46-11 delete wac user

Purpose

To delete a Web-based Access Control account.

Format

delete wac [user <username 15> | all users]

Description

This command is used to delete an account.

Parameters

Parameters	Description
username	User account for Web-based Access Control.
all users	Select this option to delete all current WAC users.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a WAC account:

```
DGS-3200-10:4#delete wac user duhon
Command: delete wac user duhon

Success.

DGS-3200-10:4#
```

46-12 config wac user

Purpose

To configure the VLAN ID of the user account.

Format

config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>| clear_vlan]

Description

This command is used to change the VLAN associated with a user.

Parameters

Parameters	Description
username	The name of user account which will change its VID.
vlan	The authentication VLAN name.
clear_vlan	Choose to clear the specified VLAN.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the port state:

```
DGS-3200-10:4# config wac user vlanid 100
Command: config wac user vlanid 100


Success.


DGS-3200-10:4#
```

46-13 show wac

Purpose

To display the Web authentication global setting.

Format

show wac

Description

This command is used to display the Web authentication global setting.

Parameters

None.

Restrictions

None.

Examples

To show WAC:

```
DGS-3200-10:4# show wac
Command: show wac

Web-Base Access Control
--------------------------------
State                     : Enabled
Method                    : RADIUS
Authentication Failover : Enabled
Redirect Path             : http://www.dlink.com
Virtual IP                : 0.0.0.0
Switch HTTP Port          : 80 (HTTP)

DGS-3200-10:4#
```

46-14 show wac ports

Purpose

To display the Web authentication port level setting.

Format

show wac ports {<portlist>}

Description

This command is used to display the port level setting.

Parameters

Parameters	Description
ports	A range of member ports to show the status.

Restrictions

None.

Examples

To show WAC ports 1 to 3:

```
DGS-3200-10:4# show wac ports 1-3
Command: show wac ports 1-3

Port         State           Aging Time      Idle Time         Block Time
                              (Minutes)        (Minutes)        (Seconds)
-------     --------       ------------      ----------      -----------
1           Disabled       1440              Infinite        60
2           Disabled       1440              Infinite        60
3           Disabled       1440              Infinite        60

DGS-3200-10:4#
```

46-15 show wac user

Purpose

To display Web authentication user accounts.

Format

show wac user

Description

This command is used to display Web authentication accounts.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show Web authentication user accounts:

```
DGS-3200-10:4# show wac user
Command: show wac user
Username        Password    VLAN ID
---------       ----------  ----------
123             abcde       1000

Total Entries    : 1

DGS-3200-10:4#
```

46-16 show wac auth_state

Purpose

To display the authentication state of a port.

Format

show wac auth_state ports {<portlist>} {authenticated | authenticating | blocked }

Description

This command is used to display the authentication state for ports.

Parameters

Parameters	Description
ports	Specifies the list of ports whose WAC state will be displayed.
authenticated	Specifies to display all authenticated users for a port.
authenticating	Specifies to display all authenticating users for a port.
blocked	Specifies to display all blocked users for a port.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the port authentication status of ports 2 to 4:

```
 DGS-3200-10:4# show wac auth_state ports 2-4
 Command: show wac auth_state ports 2-4
 Port Hosts                  VID  Aging        Idle        Block
 Time        Time         Time     Status
 ---- -------------------  ---- --------- ---------  ------  ----------------
 2     00-00-00-00-00-04     44    30           40          -
Authenticated
 3     00-00-00-00-00-01     5     98           50          -
Authenticated
 3     00-00-00-00-00-02     -      -            -           -
Authenticating
 3     00-00-00-00-00-03     -      -            -          100      Blocked
 4     00-00-00-00-00-08(P)  -      -            -           -
Authenticating

 Total Authenticating Hosts :1
 Total Authenticated Hosts  :1
 Total Blocked Hosts         :1
```

```
DGS-3200-10:4#
```

46-17 clear wac auth_state

Purpose

To clear the WAC authentication state of a port.

Format

clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr> }]

Description

This command is used to clear the authentication state of a port. The port will return to un-authenticated state. All the timer associated with the port will be reset.

Parameters

Parameters	Description
ports	Specifies the list of ports whose WAC state will be cleared.
authenticated	Specifies to clear all authenticated users for a port.
authenticating	Specifies to clear all authenticating users for a port.
blocked	Specifies to clear all blocked users for a port.
macaddr	Specifies to clear a specific user.

Restrictions

Only Administrator-level users can issue this command.

Example

To clear the WAC state of ports 1 to 5:

```
DGS-3200-10:4# clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5


Success.


DGS-3200-10:4#
```

47 MAC-based Access Control Command Lists

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]

confg mac_based_access_control guest_vlan ports <portlist>

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | hold_time [infinite | <sec 1-300>] }

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_contro auth_mac [ports [all | portlist] | mac_addr <macaddr>]

create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid < vlanid 1-4094>]}

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid < vlanid 1-4094>| clear_vlan]

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid < vlanid 1-4094>]]

show mac_based_access_control auth_mac {ports <portlist>}

show mac_based_access_control {port[<portlist> | all]}

show mac_based_access_control_local {[mac<macaddr> | vlan <vlan_name 32> | vlanid <1-4094>]}

47-1 enable mac_based_access_control

Purpose

To enable MAC-based Access Control.

Format

enable mac_based_access_control

Description

This command is used to enable the MAC-based Access Control function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable MAC-based Access Control:

```
DGS-3200-10:4# enable mac_based_access_control
Command: enable mac_based_access_control


Success.


DGS-3200-10:4#
```

47-2 disable mac_based_access_control

Purpose

To disable MAC-based Access Control.

Format

disable mac_based_access_control

Description

This command is used to disable the MAC-based Access Control function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable MAC-based Acces Control:

```
DGS-3200-10:4# disable mac_based_access_control
Command: disable mac_based_access_control


Success.


DGS-3200-10:4#
```

47-3 config mac_based_access_control password

Purpose

To configure the password of the MAC-based Access Control.

Format

config mac_based_access_control password <passwd 16>

Description

This command is used to set the password that will be used for authentication via RADIUS server.

Parameters

Parameters	Description
<passwd 16>	In RADIUS mode, the switch communicates with the RADIUS server using this password. The maximum length of the key is 16.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the password “rosebud” that will be used for authentication via RADIUS server:

```
DGS-3200-10:4# config mac_based_access_control password rosebud
Command: config mac_based_access_control password rosebud


Success.


DGS-3200-10:4#
```

47-4 config mac_based_access_control method

Purpose

To configure the MAC-based Access Control authenticating method.

Format

config mac_based_access_control method [local | radius]

Description

This command is used to authenticate via a local database or a RADIUS server.

Parameters

Parameters	Description
local	Specify to authenticate via local database.
radius	Specify to authenticate via RADIUS server.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the MAC-based Access Control method as local:

```
DGS-3200-10:4# config mac_based_access_control method local
Command: config mac_based_access_control method local


Success.


DGS-3200-10:4#
```

47-5 config mac based_access_control guest_vlan

Purpose

To configure the MAC-based Access Control guest VLAN membership.

Format

confg mac_based_access_control guest_vlan ports <portlist>

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.

Parameters

Parameters	Description
<portlist>	When the guest VLAN is configured for a port, the port will do the VLAN assignment based on the assigned VLAN from the RADIUS server. When the guest VLAN is not configured, the port will not do the VLAN assignment.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the MAC-based Access Control guest VLAN membership for port 1 to 8:

```
DGS-3200-10:4# config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8


Success.


DGS-3200-10:4
```

47-6 config mac_based_access_control ports

Purpose

To configure the MAC-based Access Control parameters.

Format

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | hold_time [infinite | <sec 1-300>] }

Description

This command is used to configure the MAC-based Access Control setting. When the MAC-AC function is enabled for a port, and the guest VLAN function for this port is disabled, the user attached to this port will not be forwarded unless the user passes the authentication. The 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 original VLAN configuration. Therefore, if the RADIUS server assigns a VLAN, the VLAN will be ignored. When the MAC-AC function is enabled for a port, and the guest VLAN function for this port is enabled, it will move from the original VLAN member port, and become a member port of the guest VLAN before the authentication process starts. After the authentication, if a valid VLAN is assigned by the RADIUS server, this port will then be removed from the guest VLAN and become a member port of the assigned VLAN.

For guest VLAN mode, there are two situations that need to be considered. If a device supports port-based VLAN classification only, 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 device supports MAC-based VLAN classification, then each user will be authorized individually and will be capable of getting its own VLAN.

For guest VLAN mode, if the MAC address is authorized, but no VLAN information is assigned from a RADIUS Server or the VLAN assigned by RADIUS server is invalid (e.g. the assigned VLAN does not exist), this port/MAC will be removed from member port of the guest VLAN and it will become a member port of the original VLAN.

Parameter

Parameters	Description
ports	A range of ports to enable or disable the MAC-based Access Control function.
state	Specify whether the MAC AC function is enabled or disabled.
mode	Either port-based or host-based. **port_based** means that all users connected to a port share the first authentication result. **host_based**: means that each user can have its own authentication result. If the switch doesn't support MAC-based VLAN, then the switch will not allow the option **host_based** for ports that are in guest VLAN mode.
method	Specify which authenticated method
aging_time	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.
hold_time	If a host fails to pass the authentication, the next authentication will not start within this time unless the user clears the entry state manually.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the port state for ports 1 to 8:

```
DGS-3200-10:4# config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable


Success.


DGS-3200-10:4#
```

47-7 create mac_based_access_control guest_vlan

Purpose

To assign a guest VLAN.

Format

create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <1-4094>]

Description

This command is used to assign a guest VLAN.

Parameters

Parameters	Description
guest_vlan	If the MAC address is authorized, the port will be assigned to this VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a MAC local:

```
 DGS-3200-10:4# 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-3200-10:4#
```

47-8 delete mac_based_access_control guest_vlan

Purpose

To de-assign a guest VLAN.

Format

delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <1-4094>]

Description

This command is used to de-assign a guest VLAN. When a guest VLAN is de-assigned, the guest VLAN function is disabled.

Parameters

Parameters	Description
vlan	Delete database with this VLAN name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To de-assign a guest VLAN:

```
DGS-3200-10:4# delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default


Success.


DGS-3200-10:4#
```

47-9 clear mac_based_access_control auth_mac

Purpose

To reset the current state of a user. The re-authentication will be started after the user traffic is received again.

Format

clear mac_based_access_contro auth_mac [ports [all | portlist] | mac_addr <macaddr>]

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.

Parameters

Parameters	Description
ports	To specify the port range to delete MAC on them.
<macaddr>	To delete a specified host with this MAC.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear the MAC being processed by MAC-based Access Control:

```
DGS-3200-10:4# clear mac_based_access_control ports all
Command: clear mac_based_access_control_ports all


Success.


DGS-3200-10:4#
```

47-10 create mac_based_access_control_local

Purpose

To create the local database entry.

Format

create mac_based_access_control_local mac <macaddr> {[vlan < vlan_name 32> | vlanid <1-4094>]}

Description

This command is used to create a database entry.

Parameters

Parameters	Description
mac	The MAC address that access accepts by local mode.
vlan	If the MAC address is authorized, the port will be assigned to this VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a local database entry:

```
 DGS-3200-10:4# 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-3200-10:4#
```

47-11 config mac_based_access_control_local

Purpose

To configure the local database entry.

Format

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <1-4094>|clear_vlan]

Description

This command is used to modify a database entry

Parameters

Parameters	Description
mac	The MAC address that access accept by local mode
vlan	If the MAC address is authorized, the port will be assigbed to this vlan.
clear_vlan	Choose to clear the specified VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure MAC-based Acess Control local:

```
 DGS-3200-10::4# 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-3200-10:4#
```

47-12 delete mac_based_access_control_local

Purpose

To delete the local database entry.

Format

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <1-4094>]

Description

This command is used to delete a database entry

Parameters

Parameters	Description
mac	Delete database by this MAC address.
vlan	Delete database by this VLAN name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a MAC-based Access Control local by MAC address:

```
DGS-3200-10:4# 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-3200-10:4#
```

To delete a MAC-based Access Control local by VLAN name:

```
DGS-3200-10:4# delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default


Success.


DGS-3200-10:4#
```

47-13 show mac_based_access_control

Purpose

To display the MAC-based Access Control setting.

Format

show mac_based_access_control {port [<portlist> | all]}

Description

This command is used to display the MAC-based Access Control setting.

Parameters

Parameters	Description
	Display the MAC-based Access Control global setting.
port	Display the MAC-based Access Control port state.

Restrictions

None.

Examples

To display MAC-based Access Control:

```
DGS-3200-10:4# show mac_based_access_control
Command: show mac_based_access_control


MAC Based Access Control
------------------------------------
State                   : Disabled
Method                  : Local
Password                : default
Guest VLAN              :
Guest VLAN Member Ports :


DGS-3200-10:4#
```

To display MAC-based Access Control for ports 1 to 4:

```
DGS-3200-10:4# show mac_based_access_control port 1-4
Command: show mac_based_access_control ports 1-4


Port     State       Aging Time    Hold Time    Auth Mode
                       (mins)       (secs)
------   --------    ----------    ---------    -----------
1       Disabled    1440          300          Host_based
2       Disabled    1440          300          Host_based
3       Disabled    1440          300          Host_based
4       Disabled    1440          300          Host_based


DGS-3200-10:4#
```

47-14 show mac_based_access_control auth_mac

Purpose

To display MAC-based Access Control authentication MAC addresses.

Format

show mac_based_access_control auth_mac {ports <portlist>}

Description

This command is used to display authentication MAC addresses on some ports or all ports.

Parameters

Parameters	Description
ports	The ports that you want to show.

Restrictions

None.

Examples

To show MAC-based Access Control authenticated MAC addresses:

```
DGS-3200-10:4# show mac_based_access_control auth_mac
Command: show mac_based_access_control auth_mac


Port Number : 1
Index  MAC Address        Auth State      VLAN Name          VID
-----  -----------------  --------------  -----------------  -----











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

47-15 show mac_based_access_control_local

Purpose

To display MAC-based Access Control local databases.

Format

show mac_based_access_control_local {[mac<macaddr>|vlan <vlan_name 32> | vlanid <1-4094>]}

Description

This command is used to display all MAC-based Access Control local databases.

Parameters

Parameters	Description
	Display all MAC-based Access Control local databases.
mac	Display MAC-based Access Control local databases by this MAC address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display MAC-based Access Control local:

```
DGS-3200-10:4# show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address                    VLAN Name                VID
-----------------  --------------------------------     ------
00-00-00-00-00-01  default                               1

Total Entries:1

DGS-3200-10:4#
```

To display MAC-based Access Control local by MAC address:

```
DGS-3200-10:4# 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                    VLAN Name              VID
-----------------  --------------------------------   ------
00-00-00-00-00-01  default                             1

Total Entries:1

DGS-3200-10:4#
```

To display MAC-based Access Control local by VLAN:

```
DGS-3200-10:4# show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address                     VLAN Name             VID
-----------------  --------------------------------   ------
00-00-00-00-00-01  default                             1

Total Entries: 1

DGS-3200-10:4#
```

48 JWAC Command List

```
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 redirect {destination [quarantine_server | jwac_login_page] | delay_time <sec 0-10>}
config jwac virtual_ip <ipaddr>
config jwac quarantine_server_url <string 128>
config jwac clear_quarantine_server_url
config jwac update_server [add | delete] ipaddress <network_address>
config jwac switch_http_port < tcp_port_number 1-65535> {[http | https]}
config jwac port [<portlist>| all] {state [enable | disable] | mode [host_based | port_based ]
|max_authenticating_host <value 0-10> | aging_time [infinite | <min 1-1440>] | idle_time [infinite |
<min 1-1440>] | block_time [<sec 0-300>]}
config jwac radius_protocol [local | pap | chap | ms_chap | ms_chapv2 | eap_md5]
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
delete jwac host [ports [all | portlist] {authenticated | authenticating | blocked} | <macaddr>]
show jwac
show jwac host {ports [all | <portlist>] } {authenticated | authenticating | blocked}
show jwac port [all | <portlist>]
config jwac authenticate_page [japanese |english]
config jwac page_element [japanese|english] [default|page_title <mutiword 128>|login_window_title
<mutiword 32>| user_name_title < mutiword 16>|password_title <mutiword 16>|
logout_window_title <mutiword 32>]
show jwac customize_page element
```

48-1 enable jwac

Purpose

To enable the JWAC function.

Format

enable jwac

Description

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable JWAC:

```
DGS-3200-10:4# enable jwac
Command: enable jwac

Success.

DGS-3200-10:4#
```

48-2 disable jwac

Purpose

To disable the JWAC function.

Format

disable jwac

Description

This command is used to disable JWAC.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable JWAC:

```
DGS-3200-10:4# disable jwac
Command: disable jwac


Success.


DGS-3200-10:4#
```

48-3 enable jwac redirect

Purpose

To enable the JWAC redirect function.

Format

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.

Parameters

None.

Restrictions

When enable redirect to quarantine server is in effect, a quarantine server must be configured first. Only Administrator-level users can issue this command.

Example

To enable JWAC redirect:

```
DGS-3200-10:4# enable jwac redirect
Command: enable jwac redirect


Success.


DGS-3200-10:4#
```

48-4 disable jwac redirect

Purpose

To disable the JWAC redirect function.

Format

disable jwac redirect

Description

This command is used to disable JWAC. 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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable JWAC redirect:

```
DGS-3200-10:4# disable jwac redirect
Command: disable jwac redirect


Success.


DGS-3200-10:4#
```

48-5 enable jwac forcible_logout

Purpose

To enable the JWAC forcible logout function.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable JWAC forcible logout:

```
DGS-3200-10:4# enable jwac forcible_logout
Command: enable jwac forcible_logout


Success.


DGS-3200-10:4#
```

48-6 disable jwac forcible_logout

Purpose

To disable the JWAC forcible logout function.

Format

disable jwac forcible_logout

Description

This command is used to disable JWAC forcible logout.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable JWAC forcible logout:

```
DGS-3200-10:4# disable jwac forcible_logout
Command: disable jwac forcible_logout

Success.

DGS-3200-10:4#
```

48-7 enable jwac udp_filtering

Purpose

To enable the JWAC UDP filtering function.

Format

enable jwac udp_filtering

Description

When UDP filtering is enabled, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable JWAC UDP filtering:

```
DGS-3200-10:4# enable jwac udp_filtering
Command: enable jwac udp_filtering

Success.

DGS-3200-10:4#
```

48-8 disable jwac udp_filtering

Purpose

To disable the JWAC UDP filtering function.

Format

disable jwac udp_filtering

Description

This command is used to disable JWAC UDP filtering.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable JWAC UDP filtering:

```
DGS-3200-10:4# disable jwac udp_filtering
Command: disable jwac udp_filtering


Success.


DGS-3200-10:4#
```

48-9 enable jwac quarantine_server_monitor

Purpose

To enable the JWAC quarantine server monitor function.

Format

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.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable JWAC quarantine server monitoring:

```
DGS-3200-10:4# enable jwac quarantine_server_monitor
Command: enable jwac quarantine_server_monitor

Success.

DGS-3200-10:4#
```

48-10 disable jwac quarantine_server_monitor

Purpose

To disable the JWAC quarantine server monitor function.

Format

disable jwac quarantine_server_monitor

Description

This command is used to disable JWAC quarantine server monitoring.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable JWAC quarantine server monitoring:

```
DGS-3200-10:4# disable jwac quarantine_server_monitor
Command: disable jwac quarantine_server_monitor

Success.

DGS-3200-10:4#
```

48-11 config jwac quarantine_server_error_timeout

Purpose

To set the quarantine server error timeout.

Format

config jwac quarantine_server_error_timeout <sec 5-300>

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.

Parameters

Parameters	Description
<sec 5-300>	Specifies the error timeout interval.

Restrictions

Only Administrator-level users can issue this command.

Example

To set the quarantine server error timeout:

```
DGS-3200-10:4# config jwac quarantine_server_error_timeout 60
Command: config jwac quarantine_server_error_timeout 60

Success.

DGS-3200-10:4#
```

48-12 config jwac redirect

Purpose

To configure redirect destination and delay time before an unauthenticated host is redirected to the quarantine server or JWAC login web page.

Format

config jwac redirect {destination [quarantine_server | jwac_login_page] | delay_time <sec 0-10>}

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.

Parameters

Parameters	Description
destination	Specifies the destination which the unauthenticated host will be redirected to.
delay_time	Specifies the time interval after which the

	unauthenticated host will be redirected.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure redirect destination and delay time before an unauthenticated host is redirected to the quarantine server or JWAC login web page:

```
DGS-3200-10:4# config jwac redirect destination jwac_login_page delay_time 5
Command: config jwac redirect_ destination jwac_login_page delay_time 5


Success.


DGS-3200-10:4#
```

48-13 config jwac virtual_ip

Purpose

To configure JWAC virtual IP addresses used to accept authentication requests from an unauthenticated host.

Format

config jwac virtual_ip <ipaddr>

Description

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.

Parameters

Parameters	Description
<ipaddr>	Specifies the IP address of the virtual IP.

Restrictions

Only Administrator-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-3200-10:4# config jwac virtual_ip 1.1.1.1
Command: config jwac virtual_ip 1.1.1.1


Success.


DGS-3200-10:4#
```

48-14 config jwac quarantine_server_url

Purpose

To configure the JWAC quarantine server URL.

Format

config jwac quarantine_server_url <string 128>

Description

This command is used to configure the URL of the quarantine server. If the redirect is enabled and the redirect destination is the quarantine server, when an HTTP request from unauthenticated host not to the quarantine server reaches the JWAC Switch, the Switch will handle this HTTP packet and send back a message to the host ot make it access the quarantine server with the configured URL. When the PC connects to the specified URL, the quarantine server will request the PC user to input the user name and password to do authentication.

Parameters

Parameters	Description
<string 128>	Specifies the entire URL of the authentication page on the Quarantine Server.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the JWAC quarantine server URL:

```
DGS-3200-10:4# 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-3200-10:4#
```

48-15 config jwac clear_quarantine_server_url

Purpose

To clear the quarantine server configuration.

Format

config jwac clear_quarantine_server_url

Description

This command is used tol clear the quarantine server configuration.

Parameters

None.

Restrictions

When JWAC is enabled and the redirect destination is the quarantine server, the quarantine server cannot be cleared. Only Administrator-level users can issue this command.

Example

To clear the quarantine server configuration:

```
DGS-3200-10:4# config jwac clear_quarantine_server_url
Command: config jwac clear_quarantine_server_url


Success.


DGS-3200-10:4#
```

48-16 config jwac update_server

Purpose

To configure the servers that the PC may need to connect to in order to complete the JWAC authentication.

Format

config jwac update_server [add | delete] ipaddress <network_address>

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.

Parameters

Parameters	Description
add	Adds a network address to which the traffic will not be blocked. Five network addresses can be added at most.
delete	Deletes a network address to which the traffic will not be blocked.
ipaddress	Specifies the network address to add or delete.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure servers the PC may need to connect to in order to complete JWAC authentication:

```
DGS-3200-10:4# config jwac other_server add ipaddress 10.90.90.109/24
Command: config jwac other_server add ipaddress 10.90.90.109/24

 Warning: the real added update server is 10.90.90.0/24

Success.

DGS-3200-10:4#
```

48-17 config jwac switch_http_port

Purpose

To configure the TCP port which the JWAC switch listens to.

Format

config jwac switch_http_port < tcp_port_number 1-65535> {[http | https]}

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.

Parameters

Parameters	Description
<tcp_port_number 1-65535>	A TCP port which the JWAC Switch listens to and uses to finish the authenticating process.
http	Specifies the JWAC run HTTP protocol on this TCP port.
https	Specifies the JWAC run HTTPS protocol on this TCP port.

Restrictions

HTTP cannot run on TCP port 443, and HTTPS cannot run on TCP port 80. Only Administrator-level users can issue this command.

Example

To configure the TCP port which the JWAC switch listens to:

```
DGS-3200-10:4# config jwac switch_http_port 8888 http
Command: config jwac switch_http_port 8888 http


Success.


DGS-3200-10:4#
```

48-18 config jwac port

Purpose

To configure the port state of JWAC.

Format

config jwac port [<portlist>| all] {state [enable | disable] | mode [host_based | port_based] |max_authenticating_host <value 0-10> | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}

Description

This command is used to configure port state of JWAC. The default value of the **max_authenticating_host** is 10. The default value of the **aging_time** is 1440 minutes. The default value of the **idle_time** is infinite. The default value of the **block_time** is 0 seconds.

Parameters

Parameters	Description
<porlist>	A port range for setting the JWAC state.
all	Every Switch ports' JWAC state is configured.
state	Specifies the port state of JWAC.
mode	Toggle between **host_based** and **port_based**.

max_authenticating_host	The maximum number of hosts that can process authentication on each port at the same time.
aging_time	A time period during which an authenticated host will keep in authenticated state. **infinite** indicates never aging out the authenticated host on the port.
idle_time	If there is no traffic during idle time, the host will be moved back to unauthenticated state. **infinite** indicates never checking the idle state of the authenticated host on the port.
block_time	If a host fail to pass the authentication, it will be blocked for a period specified by the block time.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the JWAC port state:

```
DGS-3200-10:4# config jwac port 1-9 state enable
Command: config jwac port 1-9 state enable


Success.


DGS-3200-10:4#
```

48-19 config jwac radius_protocol

Purpose

To configure the RADIUS protocol used by JWAC.

Format

config jwac radius_protocol [local | pap | chap | ms_chap | ms_chapv2 | eap_md5]

Description

This command is used to specify the RADIUS protocol used by JWAC to complete RADIUS authentication.

Parameters

Parameters	Description
local	JWAC Switch uses local user DB to complete the authentication.
pap	JWAC Switch uses PAP to communicate with the RADIUS Server.
chap	JWAC Switch uses CHAP to communicate with the RADIUS Server.
ms_chap	JWAC Switch uses MS-CHAP to communicate with the RADIUS

	Server.
ms_chapv2	JWAC Switch uses MS-CHAPv2 to communicate with the RADIUS Server.
eap_md5	JWAC Switch uses EAP MD5 to communicate with the RADIUS Server.

Restrictions

JWAC shares other RADIUS configurations with 802.1x. When using this command to set the RADIUS protocol, you must make sure the RADIUS server added by the **config radius** command supports the protocol. Only Administrator-level users can issue this command.

Example

To configure the RADIUS protocol used by JWAC:

```
DGS-3200-10:4# config jwac radius_protocol ms_chapv2
Command: config jwac radius_protocol ms_chapv2


Success.


DGS-3200-10:4#
```

48-20 create jwac user

Purpose

To create a JWAC user in the local DB.

Format

create jwac user <username 15> {vlan <vlanid 1-4094>}

config jwac user <username 15> {vlan <vlanid 1-4094>}

Description

This command creates JWAC users in the local DB. When “local” is chosen while configuring the JWAC RADIUS protocol, the local DB will be used.

Parameters

Parameters	Description
<username 15>	The user name to be created.
<vlanid 1-4094>	Target VLAN ID for authenticated host which uses this user account to pass authentication.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a JWAC user in the local DB:

```
DGS-3200-10:4# create jwac user 112233
Command: create jwac user 112233

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

DGS-3200-10:4#
```

48-21 delete jwac user

Purpose

To delete a JWAC user into the local DB.

Format

delete jwac [user <username 15> | all_users]

Description

This command is used to delete JWAC users from the local DB.

Parameters

Parameters	Description
user	Specifies the user name to be deleted
all_users	All user accouts in local DB will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a JWAC user from the local DB:

```
DGS-3200-10:4# delete jwac user 112233
Command: delete jwac user 112233

Success.

DGS-3200-10:4#
```

48-22 show jwac user

Purpose

To display a JWAC user in the local DB.

Format

show jwac user

Description

This command is used to display JWAC users in the local DB.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the current JWAC users in the local DB:

```
 DGS-3200-10:4# show jwac user
 Command: show jwac user

Current Accounts:
 Username          Target VID  Password
 ----------------  ----------  ----------------
 1                          -          1

 Total Entries:1

 DGS-3200-10:4#
```

48-23 delete jwac host

Purpose

To delete the host on JWAC enabled ports.

Format

delete jwac host [ports [all | <portlist>] {authenticated | authenticating | blocked} | <macaddr>]

Description

This command is used to delete a JWAC host.

Parameters

Parameters	Description
ports	Specifies the port range to delete the host on.
authenticated	Specifies the state of the host to delete.
authenticating	Specifies the state of host to delete.
blocked	Specifies the state of host to delete.
<macaddr>	Deletes a specified host with this MAC.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a JWAC host:

```
DGS-3200-10:4# delete jwac host ports all blocked
Command: delete jwac host ports all blocked


Success.


DGS-3200-10:4#
```

48-24 show jwac

Purpose

To display the JWAC configuration.

Format

show jwac

Description

This command is used to display the JWAC configuration settings.

Parameters

None.

Restrictions

None.

Example

To display the current JWAC configuration:

```
DGS-3200-10:4# show jwac
Command: show jwac

State                   : Enabled
Enabled Ports           : 1,9
Virtual IP              : 1.1.1.1
Switch HTTP Port        : 21212 (HTTP)
UDP Filtering           : Enabled
Forcible Logout         : Enabled
Redirect State          : Enabled
Redirect Delay Time     : 3 Seconds
Redirect Destination    : Quarantine Server
Quarantine Server       : http://172.18.212.147/pcinventory
Q-Server Monitor        : Enabled (Running)
Q-Svr Error Timeout     : 5 Seconds
Radius Auth-Protocol    : PAP
Update Server           : 172.18.202.1/32
                          172.18.202.0/24
                          10.1.1.0/24

DGS-3200-10:4#
```

48-25 show jwac host

Purpose

To display JWAC client host information.

Format

show jwac host {port [all | <portlist>]} {authenticated | authenticating | blocked}

Description

This command is used to display JWAC client host information.

Parameters

Parameters	Description
port	A port range to show the information of client host
authenticated	Only show authenticated client hosts.
authenticating	Only show client hosts in the authenticating process.
blocked	Only show client hosts being temporarily blocked because of the failure of authentication.

Restrictions

None.

Example

To display JWAC host information for port 3:

```
DGS-3200-10:4# show jwac host port 3
Command: show jwac host port 3

                                 Remaining
Hosts               Port VID  AgeTime/IdleTime   Authentication State
                              or BlockingTime
-----------------  ---- ---  ----------------   --------------------
00-00-00-00-00-01  3     5    98   Min/Infinite  Authenticated
00-00-00-00-00-02  3     99   Infinite/Infinite  Authenticating
00-00-00-00-00-03  2     44       30 Sec         Blocked

Total Authenticating Hosts :1
Total Authenticated Hosts  :1
Total Blocked Hosts        :1

DGS-3200-10:4#
```

48-26 show jwac port

Purpose

To display the port configuration of JWAC.

Format

show jwac port [all | <portlist>]

Description

This command is used to display the port configuration of JWAC.

Parameters

Parameters	Description
all	Shows all the ports configured for JWAC.
<portlist>	Specifies a port range to show the configuration of JWAC.

Restrictions

None.

Example

To display JWAC ports 1 to 4:

```
DGS-3200-10:4# show jwac port 1-4
Command: show jwac port 1-4

Port  State          Max         Aging Time Idle Time Block Time
               Authenticating  (Minutes)  (Minutes) (Seconds)
                    Host
----- -------- --------------- ---------- --------- ----------
1     Enabled       10         Infinite   20        10
2     Disabled      50         60         10        2
3     Enabled       50         1440       Infinite  2
4     Enabled       0          600        30        5

DGS-3200-10:4#
```

48-27 config jwac authenticate_page

Purpose

To customize the authenticate page.

Format

config jwac authenticate_page [japanese |english]

Description

This command is used to customize the JWAC authenticate page.

Parameters

Parameters	Description
japanese	Change to Japanese page.
english	Change to English page.

Restrictions

Only Administrator-level users can issue this command.

Example

To customize the authenticate page:

```
DGS-3200-10:4#config jwac authenticate_page japanese
Command: config jwac authenticate_page japanese


Success.


DGS-3200-10:4#
```

48-28 config jwac page_element

Purpose

To customize the authenticate page.

Format

config jwac authentication_page element [japanese|english] [default|page_title <multiword 128> |login_window_title <mutiword 32>| user_name_title <mutiword16>|password_title <mutiword 16>|logout_window_title <mutiword 32>]

Description

This command is used by administrators to customize the JWAC authenticate page.

Parameters

Parameters	Description
japanese	Change to Japanese page.
english	Changeto English page.
default	Reset the page element to default.
page_title	The title of the authenticate page.
login_window_title	The login window title of the authenticate page.
uesr_name	The user name title of the authenticate page.
password	The password title of the authenticate page.
logout_windown_title	The logout windown title mapping of the authenticate page.

Restrictions

Only Administrator-level users can issue this command.

Example

To customize the authenticate page:

```
 DGS-3200-10: config jwac page_element japanese page_title "ディーリンクジャパン株式会社
 " login_window_title "JWAC认证" user_name_title "ユーザ名" password_title "パスワ
ード" logout_window_title "ログアウト"
 Command: config jwac page_element japanese page_title "ディーリンクジャパン株式会社" log
 in_window_title "JWAC认证" user_name_title "ユーザ名" password_title "パスワード"
logout_window_title "ログアウト"

 Success.

 DGS-3200-10:
```

48-29 show jwac customize_page element

Purpose

To show the element mapping of the customize authenticate page.

Format

show jwac authenticate_page element.

Description

This command is used to display the element mapping of the customize authenticate page.

Parameters

None.

Restrictions

None.

Example

To display the default authentication page:

```
DGS-3200-10: show jwac authenticate _page element
Command: show jwac authenticate _page element

Current Page :English Version

English Page Element
------------------------------------------------------------
Page Title                             : D-Link Corp.
Login Windown Title                    : Authentication Login
User Name Title                        : User Name
Password Title                         : Password
Login Out Window Title                 : Logout

Japanese page element
--------------------------------------------------------------
Page Title                            :
Login Windown Title                   : 社内 LAN 認証ログイン
User Name Title                       : ユーザ ID
Password Title                        : パスワード
Login Out Window Title                : 社内 LAN 認証ログアウト

DGS-3200-10:
```

49 Multiple Authentication Command List

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add|delete] ports [<portlist> | all]
config authentication ports [<portlist>| all] {auth_mode [port_based | host_based] | multi_authen_methods [none | any | dot1x_impb | impb_jwac | impb_wac]}
show authentication guest_vlan
show authentication ports {<portlist>}
enable authorization network
disable authorization network
show authorization

49-1 create authentication guest_vlan

Purpose

To assign a static VLAN to be a guest VLAN.

Format

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

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.

For further description of this command, please see the description for **config authentication guest_vlan ports**.

Parameters

Parameters	Description
vlan_name 32	Specify the guest VLAN by VLAN name.
vlanid	Specify the guest VLAN by VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Example

To assign a static VLAN to be a guest VLAN:

```
DGS-3200-10:4# create authentication guest_vlan vlan guestVLAN
Command: create authentication guest_vlan vlan guestVLAN

Success.

DGS-3200-10:4#
```

49-2 delete authentication guest_vlan

Purpose

To delete a guest VLAN configuration.

Format

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

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. For further description of this command, please see the description for **config authentication guest_vlan ports**.

Parameters

Parameters	Description
vlan_name 32	Specify the guest VLAN by VLAN name.
vlanid	Specify the guest VLAN by VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a guest VLAN setting:

```
DGS-3200-10:4# delete authentication guest_vlan vlan guestVLAN
Command: delete authentication guest_vlan vlan guestVLAN

Success.

DGS-3200-10:4#
```

49-3 config authentication guest_vlan ports

Purpose

To configure security port(s) as specified guest VLAN members.

Format

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

Description

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

Parameters

Parameters	Description
vlan_name	Assign a VLAN as a guest VLAN. The VLAN must be an existing static VLAN.
vlanid	Assign a VLAN as a guest VLAN. The VLAN must be an existing static VLAN.
add	Specifies to add a port list to the guest VLAN.
delete	Specifies to delete a port list from the guest VLAN.
portlist	Specify the configured port(s).

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4# config authentication guest_vlan vlan gv add ports all
Command: config authentication guest_vlan vlan gv add ports all

Success.

DGS-3200-10:4#
```

49-4 config authentication ports

Purpose

To configure security port(s).

Format

config authentication ports [<portlist>| all] {auth_mode [port_based | host_based] | multi_authen_methods [none | any | dot1x_impb | impb_jwac | impb_wac]}

Description

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

Parameters

Parameters	Description
portlist	Port(s) to configure.
auth_mode	**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**: Every user can be authenticated individually.
multi_authen_methods	Specifies the method for multiple authentication.
none	Multiple authentication is not enabled.
any	If any one of the authentication methods (802.1x, MBAC, and JWAC/WAC) passes, then pass.
dot1x_impb	Dot1x will be verified first, and then IMPB will be verified. Both authentications need to be passed.
impb_jwac	IMPB will be verified first, and then JWAC will be verified. Both authentications need to be passed.
impb_wac	IMPB will be verified first, and then WAC will be verified. Both authentications need to be passed.

Restrictions

Only Administrator-level users can issue this command.

Examples

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

```
DGS-3200-10:4# config authentication ports all auth_mode host_based
Command: config authentication ports all auth_mode host_based

Success.

DGS-3200-10:4#
```

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

```
DGS-3200-10:4# config authentication ports all multi_authen_methods any
Command: config authentication ports all multi_authen_methods any

Success.

DGS-3200-10:4#
```

49-5 show authentication guest_vlan

Purpose

To display the guest VLAN setting.

Format

show authentication guest_vlan

Description

This command is used to display guest VLAN information.

Parameters

None.

Restrictions

None.

Examples

To display the guest VLAN setting:

```
DGS-3200-10:4# show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID         :
Guest VLAN Member Ports:

DGS-3200-10:4#
```

49-6 show authentication ports

Purpose

To display the authentication setting on port(s).

Format

show authentication ports {<portlist>}

Description

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

Parameters

Parameters	Description
	Display multiple authentication settings of all ports.
portlist	Display multiple authentication on specific port(s).

Restrictions

None.

Example

To display the authentication settings for all ports:

```
DGS-3200-10:4# show authentication ports
Command: show authentication ports

 Port         Methods       Authorized Mode
 ----    ---------------  -------------------
 1         None               Host_based
 2         Any                Host_based
 3         802.1X_IMPB        Host_based
 4         None               Host_based
 5         None               Host_based
 6         IMPB_JWAC          Host_based
 7         None               Host_based
 8         None               Host_based
 9         802.1X_IMPB        Host_based
 10        None               Host_based

DGS-3200-10:4#
```

49-7 enable authorization

Purpose

To enable authorization.

Format

enable authorization network

Description

This command is used to enable authorization on the network. When the authorization for network is enabled, the authorization data assigned by the RADUIS server will be accepted and take effect. Authorization for the network is enabled by default.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable authorization on the network:

```
DGS-3200-10:4# enable authorization network
Command: enable authorization network


Success.


DGS-3200-10:4#
```

49-8 disable authorization

Purpose

To disable authorization.

Format

disable authorization network

Description

This command is used to disable authorization on the network. Authorization for the network is enabled by default.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable authorization on the network:

```
DGS-3200-10:4# disable authorization network
Command: disable authorization network

Success.

DGS-3200-10:4#
```

49-9 show authorization

Purpose

To display the authorization status.

Format

show authorization

Description

This command is used to display the authorization status.

Parameters

None.

Restrictions

None.

Example

To display the authorization status:

```
DGS-3200-10:4#show authorization
Command: show authorization
Authorization for Network: Enabled

DGS-3200-10:4#
```

50 Filter Command List

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all] | ports [<portlist>|all] state [enable|disable]] option I
config filter dhcp_server [add permit server_ip <ipaddr> | delete permit server_ip <ipaddr> | state [enable|disable]] option II
show filter dhcp_server
config filter dhcp_server trap_log [enable | disable]
config filter dhcp_server illegal_server_log_suppress_duration [1min | 5min | 30min]

50-1 config filter dhcp_server

Purpose

To configure the state of the function for filtering of DHCP server packets and to add or delete the DHCP server or client binding entry.

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]]

config filter dhcp_server [add permit server_ip <ipaddr> | delete permit server_ip <ipaddr> | state [enable|disable]]

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.

Parameters

Parameters	Description
ipaddr	The IP address of the DHCP server to be filtered.

macaddr	The MAC address of the DHCP client.
state	Enable or disable filter DHCP server state
portlist	The port number of filter DHCP server.

Restrictions

Only Administrator-level users can issue this command.

Example

To add an entry from the DHCP server/client filter list in the switch’s database:

```
 DGS-3200-10:4# 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-3200-10:4#
```

To configure the filter DHCP server state:

```
DGS-3200-10:4# config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

DGS-3200-10:4#
```

50-2 show filter dhcp_server

Purpose

To display the DHCP server/client filter list created on the switch.

Format

show filter dhcp_server

Description

This command is used to display the DHCP server/client filter list created on the switch.

Parameters

None.

Restrictions

None.

Example

To display the DHCP server/client filter list created on the switch:

```
DGS-3200-10:4#show filter dhcp_server
Command: show filter dhcp_server
Filter DHCP Server Trap_Log State        : Disabled
Enabled Ports                           :
Illegal Server Log Suppress Duration    : 5 minutes


Filter DHCP Server/Client Table
Server IP Address   Client MAC address   Port
-----------------  -------------------  ---------------
Total Entries:  0


DGS-3200-10:4#
```

50-3 config filter dhcp_server trap_log

Purpose

To enable or disable traps or logs related to DHCP server filter.

Format

config filter dhcp_server trap_log [enable | disable]

Description

This command is used to enable or disable traps or logs related to DHCP server filter.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable log and trap for a DHCP server filter event:

```
DGS-3200-10:4# config filter dhcp_server trap_log disable
Command: config filter dhcp_server trap_log disable


Success.


DGS-3200-10:4#
```

50-4 config filter dhcp_server illegal_server_log_suppress_duration

Purpose

To configure the illegal server log suppress duration.

Format

config filter dhcp_server illegal_server_log_suppress_duration [1min | 5min | 30min]

Description

This command is used to suppress the logging of DHCP servers which continue to send illegal DHCP packets. The same illegal DHCP server IP address detected will be logged only once within the duration.

Parameters

Parameters	Description
illegal _server_log_suppress_duration	The same illegal DHCP server IP address detected will be logged only once within the duration. The log can be suppressed by one minute, 5 minutes, or 30 minutes. The default value is 5 minutes.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure an illegal server log suppress duration:

```
DGS-3200-10:4# config filter dhcp_server illegal _server_log_suppress_duration
30min
Command: config filter dhcp_server illegal _server_log_suppress_duration 30min


Success.
DGS-3200-10:4#
```

IX. QoS

The QoS section includes the following chapter: QoS.

51 QoS Command List

config bandwidth_control [<portlist>|all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}

show bandwidth_control {<portlist>}

config scheduling <class_id 0-7> max_packet<value 0-255>

config scheduling_mechanism [strict | weight_fair]

show scheduling

show scheduling_mechanism

config 802.1p user_priority <priority 0-7> <class_id 0-7>

show 802.1p user_priority

config 802.1p default_priority [<portlist> | all] <priority 0-7>

show 802.1p default_priority { <portlist>}

51-1 config bandwidth_control

Purpose

To configure the port bandwidth limit control.

Format

config bandwidth_control [<portlist>|all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit |<value 64-1024000>]}

Description

This command is used to set the maximum limit for port bandwidth.

Parameters

Parameters	Description
portlist	Specifes a range of ports to be configured.
rx_rate	Specifies the limitation of receive data rate.

	no_limit - Indicates there is no limit on port rx bandwidth. An integer value from 64 to 1024000 sets 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. The token value will always be a multiple of the bandwidth increment specific to the chip used for the project (i.e. 32 Kbits, 64 Kbits, 128 Kbits, etc.). This token value, the actual set limit recognized by the CPU, will be displayed when the user enters the bandwidth limit integer. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits.
tx_rate	Specifies the limitation of transmit data rate.
	no_limit - Indicates there is no limit on port tx bandwidth. An integer value from 64 to 1024000 sets 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. The token value will always be a multiple of the bandwidth increment specific to the chip used for the project (i.e. 32 Kbits, 64 Kbits, 128 Kbits, etc.). This token value, the actual set limit recognized by the CPU, will be displayed when the user enters the bandwidth limit integer. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure port bandwidth:

```
DGS-3200-10:4#config bandwidth_control 1-10 tx_rate 1024
Command: config bandwidth_control 1-10 tx_rate 1024


Success.


DGS-3200-10:4#
```

Response messages

(1). “**Success.**”

When users input a value that is a multiple of 64 and the setting is successful.

(2). "**Fail !**

Trunk member port can not be configured because the master is not contained in the portlist" .

The configured portlist contains trunk port but not it’s master port.

51-2 show bandwidth_control

Purpose

To display the port bandwidth control table.

Format

show bandwidth_control {<portlist>}

Description

This command is used to display the port bandwidth configurations.

Parameters

Parameters	Description
portlist	Specifies a range of ports to be displayed.
	If no parameter is specified, the system will display all port bandwidth configurations.

Restrictions

None.

Examples

To display the port bandwidth control table:

```
DGS-3200-10:4#show bandwidth_control  1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

Port   RX Rate       TX Rate      Effective RX        Effective TX
      (Kbit/sec)    (Kbit/sec)     (Kbit/sec)          (Kbit/sec)
----  ----------    ----------    ----------------    ----------------
 1    no_limit      no_limit      no_limit            no_limit
```

```
2    no_limit      no_limit      no_limit          no_limit
3    no_limit      no_limit      no_limit          no_limit
4    no_limit      no_limit      no_limit          no_limit
5    no_limit      no_limit      no_limit          no_limit
6    no_limit      no_limit      no_limit          no_limit
7    no_limit      no_limit      no_limit          no_limit
8    no_limit      no_limit      no_limit          no_limit
9    no_limit      no_limit      no_limit          no_limit
10   no_limit      no_limit      no_limit          no_limit

DGS-3200-10:4#
```

51-3 config scheduling

Purpose

To configure the traffic scheduling mechanism for each COS queue.

Format

config scheduling <class_id 0-7> max_packet <value 0-255>

Description

This command is used to configure the traffic scheduling mechanism. The switch contains n+1 hardware priority queues. Incoming packets must be mapped to one of these n+1 queues. This command is used to specify the rotation by which these n+1 hardware priority queues are emptied.

Parameters

Parameters	Description
class_id	This specifies which of the n+1 hardware priority queues the config scheduling command will apply to. The four hardware priority queues are identified by number – from 0 to n – with the 0 queue being the lowest priority.
weight	Specifies the weights for weighted fair queueing. A value between 0 and 255 can be specified.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-3200-10:4# config scheduling 0 max_packet 34
Command: config scheduling 0 max_packet 34


Success.


DGS-3200-10:4#
```

51-4 config scheduling_mechanism

Purpose

To configure the traffic scheduling mechanism for each COS queue.

Format

config scheduling_mechanism [strict | weight_fair]

Description

This command is used to specify how the switch handle packets in priority queues.

Parameters

Parameters	Description
strict	The highest queue first process.That is, the highest queue should be finished first.
weight_fair	Use weighted fair algorithm to handle packets in priority queues.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-3200-10:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict


Success.


DGS-3200-10:4#
```

51-5 show scheduling

Purpose

To display the current traffic scheduling parameters in use on the switch.

Format

show scheduling

Description

This command is used to display the current traffic scheduling parameters in use on the switch.

Parameters

None.

Restrictions

None.

Examples

To display traffic scheduling parameters for each COS queue (for ex., eight hardware priority queues):

```
DGS-3200-10:4# show scheduling
Command: show scheduling


QOS Output Scheduling


Class ID  MAX. Packets
--------  ------------
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-3200-10:4#
```

51-6 show scheduling_mechanism

Purpose

To show the traffic scheduling mechanism.

Format

show scheduling_mechanism

Description

This command is used to display the traffic scheduling mechanism.

Parameters

None.

Restrictions

None.

Examples

To show the scheduling mechanism:

```
DGS-3200-10:4# show scheduling_mechanism
Command: show scheduling_mechanism

QOS scheduling mechanism
CLASS ID  Mechanism
--------  -----------
Class-0   strict
Class-1   strict
Class-2   strict
Class-3   strict
Class-4   strict
Class-5   strict
Class-6   strict
Class-7   strict

DGS-3200-10:4#
```

51-7 config 802.1p user_priority

Purpose

To map the 802.1p user priority of an incoming packet to one of the four hardware queues available on the switch.

Format

config 802.1p user_priority <priority 0-7> <class_id 0-7>

Description

This command is used to configure the way the switch will map an incoming packet, based on its 802.1p user priority, to one of the four available hardware priority queues on the switch. The switch's default is to map the following incoming 802.1p user priority values to the four hardware priority queues.

Parameters

Parameters	Description
priority	The 802.1p user priority you want to associate with the **<class_id>** (the number of the hardware queue) with.
class_id	The number of the switch's hardware priority queue. The switch has n+1 hardware priority queues available. They are numbered between 0 (the lowest priority) and n (the highest priority).

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the 802.1p user priority:

```
DGS-3200-10:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3200-10:4#
```

51-8 show 802.1p user_priority

Purpose

To display 802.1p user priority.

Format

show 802.1p user_priority

Description

This command is used to display 802.1p user priority.

Parameters

None.

Restrictions

None.

Examples

To display the traffic scheduling mechanism for each COS queue:

```
DGS-3200-10:4# show 802.1p user_priority
Command: show 802.1p user_priority


QOS Class of Traffic
Priority-0  ->  <Class-2>
Priority-1  ->  <Class-0>
Priority-2  ->  <Class-1>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-4>
Priority-5  ->  <Class-5>
Priority-6  ->  <Class-6>
Priority-7  ->  <Class-7>


DGS-3200-10:4#
```

51-9 config 802.1p default_priority

Purpose

To configure the 802.1p default priority settings on the switch. If an untagged packet is received by the switch, the priority configured with this command will be written to the packet's priority field.

Format

config 802.1p default_priority [<portlist> | all] <priority 0-7>

Description

This command is used to specify default priority handling of untagged packets received by the switch. The priority value entered with this command will be used to determine which of the four hardware priority queues the packet is forwarded to.

Parameters

Parameters	Description
portlist	This specifies a range of ports for which the default priority is to be configured. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The beginning and end of the port list range are separated by a dash.
all	Specifies that the command applies to all ports on the switch.
priority	The priority value (0 to 7) you want to assign to untagged packets received by the switch or a range of ports on the switch.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the 802.1p default priority settings on the switch:

```
DGS-3200-10:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5


Success.


DGS-3200-10:4#
```

51-10 show 802.1p default_priority

Purpose

To display the current default priority settings on the switch.

Format

show 802.1p default_priority { <portlist> }

Description

This command is used to display the current default priority settings on the switch.

Parameters

Parameters	Description
portlist	Specified a range of ports to be displayed.
	If no parameter is specified, the system will display all ports with 802.1p **default_priority**.

Restrictions

None.

Examples

To display 802.1p default priority:

```
DGS-3200-10:4# show 802.1p default_priority
Command: show 802.1p default_priority

Port       Priority      Effective Priority
----       -----------   ------------------
1              0                 0
2              0                 0
3              0                 0
4              0                 0
5              0                 0
6              0                 0
7              0                 0
8              0                 0
9              0                 0
10             0                 0

DGS-3200-10:4#
```

X. IP Addressing Service

The IP Addressing Service section includes the following chapters: DHCP Relay and DHCP Local Relay.

52 DHCP Relay Command List

config dhcp_relay { hops <value 1-16> | time <sec 0-65535>}

config dhcp _relay [add|delete] ipif <ipif_name 12> <ipaddr>

config dhcp_relay option_82 { state [enable|disable] | check [enable|disable] | policy [replace|drop|keep] }

enable dhcp _relay

disable dhcp _relay

show dhcp _relay {ipif <ipif_name 12>}

Note: 1. 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.

2. 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.

52-1 config dhcp_relay

Purpose

To configure the DHCP relay feature of the switch.

Format

config dhcp_relay { hops <value 1-16> | time <sec 0-65535>}

Description

This command is used to configure the DHCP relay feature of the switch.

Parameters

Parameters	Description
hops	Specifies the maximum number of router hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4.
time	The minimum time in seconds within which the switch must relay the DHCP/BOOTP request. If this time is exceeded, the switch will drop the DHCP/BOOTP packet.The range is 0 to 65535. The default value is 0.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure DHCP relay status:

```
DGS-3200-10:4#config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DGS-3200-10:4#
```

52-2 config dhcp_relay add

Purpose

To add an IP destination address to the switch’s DHCP relay table.

Format

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

Description

This command is used to add an IP address as a destination to forward (relay) DHCP/BOOTP packets.

Parameters

Parameters	Description
ipif_name	The name of the IP interface which contains the IP address below.
ipaddr	The DHCP/BOOTP server IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a DHCP/BOOTP server to the relay table:

```
DGS-3200-10:4#config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DGS-3200-10:4#
```

52-3 config dhcp_relay delete

Purpose

To delete one or all IP destination addresses from the switch's DHCP relay table.

Format

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

Description

This command is used to delete one or all of the IP destination addresses in the swith's relay table.

Parameters

Parameters	Description
ipif_name	The name of the IP interface which contains the IP address below.
ipaddr	The DHCP/BOOTP server IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a DHCP/BOOTP server to the relay table:

```
DGS-3200-10:4#config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12


Success.


DGS-3200-10:4#
```

52-4 config dhcp_relay option_82

Purpose

To configure the DHCP relay agent information option 82 of the switch.

Format

config dhcp_relay option_82 { state [enable|disable] | check [enable|disable] | policy [replace|drop|keep] }

Description

This command is used to configure the DHCP relay agent information option 82 setting of the switch. The formats for the circuit ID suboption and the remote ID suboption are as following. For the circuit ID suboption of a standalone switch, the module field is always zero.

Circuit ID suboption format :

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	Module	Port
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

1. Suboption type 2. Length

3. Circuit ID type 4. Length

5. VLAN : The incoming VLAN ID of DHCP client packet.

6 . Module : For a standalone switch, Module is always 0.

7. Port : The incoming port number of DHCP client packet, port number starts from 1.

Remote ID suboption format :

1.	2.	3.	4.	5.
2	8	0	6	MAC address
1 byte	1 byte	1 byte	1 byte	6 bytes

1. Suboption type 2. Length

3. Remote ID type 4. Length

5. MAC address : The switch's system MAC address.

Parameters

Parameters	Description
state	Enable or disable the switch to insert and remove DHCP relay agent information 82 field in messages between DHCP server and client. The default setting is **disable**.
check	Enable or disable the switch to check the validity of DHCP relay agent information 82 field in messages between DHCP server and client. The invalid messages are those packets that contain the option 82 field from DHCP client and those packets that contain the wrong format of option 82 field from DHCP server. If check is set to enable, the switch will drop all invalid messages received from DHCP server or client. The default setting is **disable**.
policy	Configure the reforwarding policy as following : **replace**: replace the exiting option 82 field in messages. **drop**: discard messages with existing option 82 field. **keep**: retain the existing option 82 field in messages. The default setting is replace. Note: The reforwarding policy is active only when the "check" option is disabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the DHCP relay option 82:

```
DGS-3200-10:4#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3200-10:4#config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

DGS-3200-10:4#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3200-10:4#
```

52-5 enable dhcp_relay

Purpose

To enable the DHCP relay function on the switch.

Format

enable dhcp_relay

Description

This command is used to enable the DHCP relay function on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the DHCP relay function:

```
DGS-3200-10:4#enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3200-10:4#
```

52-6 disable dhcp_relay

Purpose

To disable DHCP relay function on the switch.

Format

disable dhcp_relay

Description

This command is used to disable the DHCP relay function on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the DHCP relay function:

```
DGS-3200-10:4#disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3200-10:4#
```

52-7 show dhcp_relay

Purpose

To display the current DHCP relay configuration.

Format

show dhcp_relay {ipif <ipif_name 12>}

Description

This command is used to display the current DHCP relay configuration.

Parameters

Parameters	Description
ipif_name	The IP interface name.
	If no parameter is specified , the system will display all DHCP relay configurations.

Restrictions

None.

Examples

To display the DHCP relay status:

```
DGS-3200-10:4# show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status          : Disabled
DHCP/BOOTP Hops Count Limit      : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State   : Disabled
DHCP Relay Agent Information Option 82 Check   : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace

Interface     Server 1        Server 2         Server 3        Server 4
------------- --------------- ---------------- --------------- --------------
System        10.48.74.122    10.23.12.34      10.12.34.12     10.48.75.121

DGS-3200-10:4#
```

53 DHCP Local Relay Command List

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

enable dhcp _local_relay

disable dhcp_relay_relay

show dhcp _local_relay

.

53-1 config dhcp_local_relay vlan

Purpose

To enable or disable the DHCP local relay function for a specific VLAN.

Format

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

Description

This command is used to enable or disable the DHCP local relay function for a specified VLAN. When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed as a broadcast without changing the source MAC address and gateway address. DHCP option 82 will be automatically added.

Parameters

Parameters	Description
vlan_name	The name of the VLAN to be enabled for DHCP local relay.
state	Enable or disable DHCP local relay for a specified VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable DHCP local relay for a default VLAN:

```
DGS-3200-10:4#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable


Success.


DGS-3200-10:4#
```

53-2 enable dhcp_local_relay

Purpose

To enable DHCP local relay.

Format

enable dhcp_local_relay

Description

This command is used to enable the DHCP local relay function on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the DHCP local relay function:

```
DGS-3200-10:4#enable dhcp_local_relay
Command: enable dhcp_local_relay


Success.


DGS-3200-10:4#
```

53-3 disable dhcp_local_relay

Purpose

To disable the DHCP local relay function.

Format

disable dhcp_local_relay

Description

This command is used to disable the DHCP local relay function on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the DHCP local relay function:

```
DGS-3200-10:4#disable dhcp_local_relay
Command: disable dhcp_local_relay


Success.


DGS-3200-10:4#
```

53-4 show dhcp_local_relay

Purpose

To display the current DHCP local relay configuration.

Format

show dhcp_local_relay

Description

This command is used to display the current DHCP local relay configuration on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display the local DHCP relay status:

```
DGS-3200-10:4#show dhcp_local_relay
Command: show dhcp_local_relay



DHCP/BOOTP Local Relay Status            : Disabled
DHCP/BOOTP Local Relay VLAN List         : 1,3-4


DGS-3200-10:4#
```

XI. IPv6

The IPv6 section includes the following chapter: IPv6 NDP.

54 IPv6 NDP Command List

create ipv6 neighbor_cache ipif <ipif_name 12>   <ipv6addr>   <macaddr>
delete ipv6 neighbor_cache ipif [<ipif_name 12>|all] [<ipv6addr> | static| dynamic| all]
show ipv6 neighbor_cache ipif [<ipif_name 12>|all] [ipv6address <ipv6addr> | static|dynamic|all]
config ipv6 nd ns ipif <ipif_name 12> retrans_timer <value 0-4294967295>
show ipv6 nd ipif {<ipif_name 12>}

54-1 delete ipv6 neighbor_cache

Purpose

To add a static neighbor on an IPv6 interface.

Format

create ipv6 neighbor_cache ipif <ipif_name 12>   <ipv6addr>   <macaddr>

Description

This command is used to add a static neighbor on an IPv6 interface

Parameters

Parameters	Description
ipif_name	The interface’s name.
ipv6addr	The address of the neighbor.
macaddr	The MAC address of the neighbor.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a static neighbor cache entry:

```
DGS-3200-10:4#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-3200-10:4#
```

54-2 delete ipv6 neighbor_cache

Purpose

To delete an IPv6 neighbor from the interface neighbor address cache.

Format

delete ipv6 neighbor_cache ipif [<ipif_name 12>|all] [<ipv6addr> | static| dynamic| all]

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 IPIF. Both static and dynamic entry can be deleted.

Parameters

Parameters	Description
Ipif_name	The IPv6 interface.
ipv6addr	The address of the neighbor.
all	All entries include static and dynamic entries will be deleted.
dynamic	Delete those dynamic entries.
static	Delete the static entry

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a neighbor cache:

```
DGS-3200-10:4#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1


Success.


DGS-3200-10:4#
```

54-3 show ipv6 neighbor_cache

Purpose

To display an IPv6 neighbor cache.

Format

show ipv6 neighbor_cache ipif [<ipif_name 12>|all] [ipv6address <ipv6addr> | static|dynamic|all]

Description

This command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all entries, and all static entries..

Parameters

Parameters	Description
<ipif_name 12>	The interface's name.
< ipv6addr>	The address of the entry.
static	Static neighbor cache entry.
dynamic	Dynamic entries.

Restrictions

None.

Examples

To display an IPv6 neighbor cache:

```
DGS-3200-10:4#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

Neighbor                     Link Layer Address  Interface    State
--------------------------  ------------------  ------------  -----
FE80::20B:6AFF:FECF:7EC6    00-0B-6A-CF-7E-C6   System         T

Total Entries: 1

State:
(I) means Incomplete state. (R) means Reachable state.
(S) means Stale state.      (D) means Delay state.
(P) means Probe state.      (T) means Static state.



DGS-3200-10:4#
```

54-4 config ipv6 nd ns

Purpose

To configure neighbor solicitation related arguments.

Format

config ipv6 nd ns ipif <ipif_name 12> retrans_timer <value 0-4294967295>

Description

This command is used to configure neighbor solicitation related arguments.

Parameters

Parameters	Description
ipif_name	The name of the interface.
ns retrans_timer	Neighbor solicitation's retransmit timer in milliseconds. It has the same value as ra retrans_time in the config ipv6 nd ra command. If we configure one, the other will change too.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure neighbor solicitation related arguments:

```
DGS-3200-10:4#config ipv6 nd ns ipif System retrans_time 400
Command: config ipv6 nd ns ipif System retrans_time 400

Success.

DGS-3200-10:4#
```

54-5 show ipv6 nd

Purpose

To display an interface's information.

Format

show ipv6 nd {ipif <ipif_name 12>}

Description

This command is used to display IPv6 ND related configuration.

Parameters

Parameters	Description
ipif_name	The interface name.

Restrictions

None.

Examples

To display an interface's information:

```
DGS-3200-10:4#show ipv6 nd ipif System
Command: show ipv6 nd ipif System



Interface Name                  : System
Hop Limit                       : 64
NS Retransmit Time              : 0 (ms)
Router Advertisement            : Disabled
RA Max Router AdvInterval       : 600 (s)
RA Min Router AdvInterval       : 198 (s)
RA Router Life Time             : 1800 (s)
RA Reachable Time               : 1200000 (ms)
RA Retransmit Time              : 0 (ms)
RA Managed Flag                 : Disabled
RA Other Config Flag            : Disabled

DGS-3200-10:4
```

XII. ACL

The ACL section includes the following chapter: ACL.

55 ACL Command List

```
create access_profile profile_id <value 1-200>
      [ ethernet
          { vlan | source_mac <macmask 000000000000-ffffffffffff> |
           destination_mac <macmask 000000000000-ffffffffffff> |
           802.1p | ethernet_type }"
     | ip
         { vlan
           source_ip_mask <netmask> |   destination_ip_mask <netmask> |   dscp |
           [icmp {type | code }   | igmp {type } |
           tcp   {src_port_mask <hex 0x0-0xffff> | dst_port_mask(<hex 0x0-0xffff> |
                 flag_mask [ all | {urg | ack | psh| rst| syn | fin} ] } |
           udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
           protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}(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> }
     | ipv6
         {class | flowlabel | source_ipv6_mask<ipv6mask> | destination_ipv6_mask <ipv6mask>}]
```

```
delete access_profile [profile_id <value 1-200> | all]
```

```
config access_profile profile_id <value 1-200>
     [ add access_id [ auto_assign | <value 1-200> ]
     [ ethernet
         {vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |
         destination_mac <macaddr 000000000000-ffffffffffff> |
         802.1p <value 0-7> |ethernet_type <hex 0x0-0xffff> }
          | ip
        { vlan <vlan_name 32> | source_ip <ipaddr> |destination_ip <ipaddr> |dscp <value 0-63> |
        [icmp {type <value 0-255>| code <value 0-255>} | igmp {type <value 0-255>} |
        tcp { src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin} |
        udp {src_port(<value 0-65535> | dst_port <value 0-65535>} |
        protocol_id <value 0 - 255>   {user_define<hex 0x0-0xffffffff>}]}
    | packet_content_mask
      {    offset_chunk_1    <hex 0x0-0xffffffff>
           offset_chunk_2   <hex 0x0-0xffffffff>
           offset_chunk_3   <hex 0x0-0xffffffff>
           offset_chunk_4   <hex 0x0-0xffffffff> }
    | ipv6   { class <value 0-255> | flowlabel <hex 0x0-0xfffff> |
        source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>} ] port [<portlist> | all ]
    [ permit { priority   <value 0-7> {replace_priority} | replace_dscp <value 0-63> | rx_rate
[ no_limit | <value 1-156249>] } | mirror | deny]
    {time_range <range_name 32>} |delete access_id <value 1-200> ]
```

```
show access_profile {profile_id <value 1-200>}
```

```
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
```

```
create cpu access_profile profile_id <value 1-5>
    [ ethernet
       { vlan | source_mac <macmask 000000000000-ffffffffffff> |
        destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}
    | ip
       { vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> |
        dscp | [icmp {type | code} | igmp {type } |
        tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> |
           flag_mask [ all | {urg | ack | psh | rst | syn| fin} ] } |
        udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
        protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}
    | packet_content_mask
        {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
         offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex
0x0-0xffffffff> |
         offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex
0x0-0xffffffff> |
         offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex
0x0-0xffffffff> |
         offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex
0x0-0xffffffff>} | ipv6
        {class | flowlabel| source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>} ]
```

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

```
config cpu access_profile profile_id <value 1-5>"
      [add access_id <value 1-100>"
        [ethernet
            {vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |
            destination_mac <macaddr 000000000000-ffffffffffff> |
            802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> }
        | ip
            {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value
0-63> |
            [   icmp {type <value 0-255> | code <value 0-255>} |
               igmp {type <value 0-255>} |
               tcp{src_port <value 0-65535> | dst_port <value 0-65535> |
                   urg | ack | psh | rst | syn | fin } |
               udp {src_port <value 0-65535> | dst_port <value 0-65535>} |
               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
```

55-1 create access_profile

Purpose

To create access list rules.

Format

```
create access_profile profile_id <value 1-200>
[ ethernet
{ vlan | source_mac <macmask 000000000000-ffffffffffff> |
 destination_mac <macmask 000000000000-ffffffffffff> |
 802.1p | ethernet_type } | ip
{ vlan
 source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp |
 [icmp {type | code }   | igmp {type } |
  tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask(<hex 0x0-0xffff> |
 flag_mask [ al | {urg | ack | psh| rst| syn | fin}] } |
 udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
 protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}
| packet_content_mask
{offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff>
offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff>
offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff>
offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6
{class | flowlabel | source_ipv6_mask<ipv6mask> | destination_ipv6_mask <ipv6mask>} ]
```

Description

This command is used to create access list rules.

Note: Please see the Appendix section entitled “Mitigating ARP Spoofing Attacks Using Packet Content ACL” for a configuration example and further information.

Parameters

Parameters	Description
vlan	Specifies a VLAN mask.
source_mac	Specifies the source MAC mask.
destination_mac	Specifies the destination MAC mask.
802.1p	Specifies 802.1p priority tag mask.
ethernet_type	Specifies the Ethernet type mask.
vlan	Specifies a VLAN mask.
source_ip_mask	Specifies an IP source submask.
destination_ip_mask	Specifies an IP destination submask.

<table>
<tr><td><b>dscp</b></td><td colspan="2">Specifies the DSCP mask.</td></tr>
<tr><td rowspan="3"><b>icmp</b></td><td colspan="2">Specifies that the rule applies to icmp traffic.</td></tr>
<tr><td><b>type</b></td><td>Specifies the ICMP packet type.</td></tr>
<tr><td><b>code</b></td><td>Specifies the ICMP code.</td></tr>
<tr><td rowspan="2"><b>igmp</b></td><td colspan="2">Specifies that the rule applies to IGMP traffic.</td></tr>
<tr><td><b>type</b></td><td>Specifies the IGMP packet type</td></tr>
<tr><td rowspan="4"><b>tcp</b></td><td colspan="2">Specifies that the rule applies to TCP traffic.</td></tr>
<tr><td><b>src_port_mask</b></td><td>Specifies the TCP source port mask.</td></tr>
<tr><td><b>dst_port_mask</b></td><td>Specifies the TCP destination port mask.</td></tr>
<tr><td><b>flag_mask</b></td><td>Specifies the TCP flag field mask.</td></tr>
<tr><td rowspan="3"><b>udp</b></td><td colspan="2">Specifies that the rule applies to UDP traffic.</td></tr>
<tr><td><b>src_port_mask</b></td><td>Specifies the TCP source port mask.</td></tr>
<tr><td><b>dst_port_mask</b></td><td>Specifies the TCP destination port mask.</td></tr>
<tr><td rowspan="2"><b>protocod_id_mask</b></td><td colspan="2">Specifies that the rule applies to the IP protocol ID traffic.</td></tr>
<tr><td><b>user_define_mask</b></td><td>Specifies the L4 part mask.</td></tr>
<tr><td><b>packet_content_mask</b></td><td colspan="2">Specifies the frame content mask. There are a maximum of five offsets that can be configured. Each offset presents 16 bytes, the range of mask of frame is 80 bytes (5 offsets) in the first eighty bytes of frame.</td></tr>
<tr><td><b>offset</b></td><td colspan="2">Specifies the mask pattern offset of frame.</td></tr>
<tr><td><b>offset_chunk_1,</b>
<b>offset_chunk_2,</b>
<b>offset_chunk_3,</b>
<b>offset_chunk_4</b></td><td colspan="2">Specifies the frame content offset and mask. Up to four trunk offset and masks in maximum can be configured. A trunk mask presents 4 bytes. Four offset chunks can be selected out from 32 predefined offset chunks as described below:
<table>
<tr><td>chunk0</td><td>chunk1</td><td>chunk2</td><td>……</td><td>chunk29</td><td>chunk30</td><td>chunk31</td></tr>
<tr><td>B126,
B127,
B0,
B1</td><td>B2,
B3,
B4,
B5</td><td>B6,
B7,
B8,
B9</td><td>……</td><td>B114,
B115,
B116,
B117</td><td>B118,
B119,
B120,
B121</td><td>B122,
B123,
B124,
B125</td></tr>
</table>
Example:
offset_chunk_1 0 0xffffffff will match packet byte offset 126,127,0,1
offset_chunk_1 0 0x0000ffff will match packet byte offset 0,1
Note: Only one packet content mask profile can be created.</td></tr>
<tr><td><b>class</b></td><td colspan="2">Specifies the IPv6 class mask.</td></tr>
<tr><td><b>flowlabel</b></td><td colspan="2">Specifies the IPv6 flow label mask.</td></tr>
<tr><td><b>source_ipv6_mask</b></td><td colspan="2">Specifies the IPv6 source IP mask.</td></tr>
<tr><td><b>destination_ipv6_mask</b></td><td colspan="2">Specifies the IPv6 destination IP mask.</td></tr>
</table>

Restrictions

Only Administrator-level users can issue this command. The Switch supports a maximum of 200 profiles.

Example

To create access list rules:

```
DGS-3200-10:4#create access_profile profile_id 100 ethernet vlan source_mac FF-F
F-FF-FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p ethernet_type
Command: create access_profile profile_id 100 ethernet vlan source_mac FF-FF-FF-
FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p ethernet_type

Success.

DGS-3200-10:4#

DGS-3200-10:4#create access_profile profile_id 101 ip vlan source_ip_mask 255.25
5.255.255 destination_ip_mask 255.255.255.0 dscp icmp
Command: create access_profile profile_id 101 ip vlan source_ip_mask 255.255.255
.255 destination_ip_mask 255.255.255.0 dscp icmp

Success.

DGS-3200-10:4#
```

55-2 delete access_profile

Purpose

To delete access list rules.

Format

delete access_profile [profile_id <value 1-200> | all]

Description

This command is used to delete access list rules.

Parameters

Parameters	Description
profile_id	Specifies the index of access list profile.
all	Specifies the whole access list profile to delete.

Restrictions

Only Administrator-level users can issue this command. The Switch supports a maximum of 200 access entries. The **delete access_profile** command can only delete the profile which is created by the ACL module.

Example

To delete access list rules:

```
DGS-3200-10:4#delete access_profile profile_id 10
Command: delete access_profile profile_id 10


Success.


DGS-3200-10:4#
```

55-3 config access_profile

Purpose

To configure access list entries.

Format

config access_profile profile_id <value 1-200> [add access_id [auto_assign | <value 1-200>]
[ethernet
{vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |
destination_mac <macaddr 000000000000-ffffffffffff> |
802.1p <value 0-7> |ethernet_type <hex 0x0-0xffff> }
| ip
{ vlan <vlan_name 32> | source_ip <ipaddr> |destination_ip <ipaddr> |dscp <value 0-63> |
[icmp {type <value 0-255>| code <value 0-255>} | igmp {type <value 0-255>} |
tcp { src_port <value 0-65535> | dst_port <value 0-65535> |
urg | ack | psh | rst | syn | fin} |
udp {src_port(<value 0-65535> | dst_port <value 0-65535>} |
protocol_id <value 0 - 255>   {user_define<hex 0x0-0xffffffff>}]}
| packet_content_mask
{offset_chunk_1   <hex 0x0-0xffffffff>
offset_chunk_2   <hex 0x0-0xffffffff>
offset_chunk_3   <hex 0x0-0xffffffff>
offset_chunk_4   <hex 0x0-0xffffffff> }
| ipv6
{ class <value 0-255> | flowlabel <hex 0x0-0xfffff> |
source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all]

[permit { priority <value 0-7> {replace_priority}| replace_dscp <value 0-63> | rx_rate [no_limit | <value 1-156249>] } | mirror | deny] {time_range <range_name 32>}
|delete access_id <value 1-200>]

Description

This command is used to configure access list entries.

Note: Please see the Appendix section entitled “Mitigating ARP Spoofing Attacks Using Packet Content ACL” for a configuration example and further information.

Parameters

Parameters	Description		
profile_id	Specifies the index of the access list profile.		
access_id	Specifies the index of the access list entry. The range of this value is 1 to 200.		
	vlan	Specifies a VLAN name.	
	source_mac	Specifies the source MAC.	
	destination_mac	Specifies the destination MAC.	
	802.1p	Specifies the value of 802.1p priority tag, the value can be configured between 1 to 7.	
	ethernet_type	Specifies the Ethernet type.	
	vlan	Spcifies a VLAN name.	
	source_ip	Specifies an IP source address.	
	destination_ip	Specifies an IP destination address.	
	dscp	Specifies the value of DSCP, the value can be configured from 0 to 63.	
	icmp	Specifies that the rule applies to ICMP traffic.	
		type	Specifies the ICMP packet type.
		code	Specifies the ICMP packet code.
	igmp	Specifies that the rule applies to IGMP traffic.	
		type	Specifies the IGMP packet type.
	tcp	**src_port**	Specifies that the rule applies the range of TCP source port.
		dst_port	Specifies the range of tcp destination port range.
		flag	Specifies the TCP flag fields .
	udp	**src_port**	Specifies the range of tcp source port range.
		dst_port	Specifies the range of tcp destination port mask.
	protocod_id	Specifies that the rule applies to the value of IP protocol id traffic	
		user_define	Specifics the L4 part value.

	offset_chunk_1, **offset_chunk 2,** **offset_chunk 3,** **offset_chunk 4**	Specifies the content of the trunk to be monitored
	class	Specifies IPv6 class value.
	flowlabel	Specifies IPv6 flow label value.
	source_ipv6	Specifies IPv6 source IP value.
	destination_ipv6	Specifies IPv6 destionation IP value.
permit	Specifies the packets that match the access profile are permit by the switch.	
priority	Specifies the packets that match the access profile are remap the 802.1p priority tag field by the switch.	
replace_priority	Specifies the packets that match the access profile remarking the 802.1p priority tag field by the switch.	
rx_rate	Specifies the limitation of receive data rate.	
replace_dscp	Specifies the DSCP of the packets that match the access profile are modified according to the value.	
deny	Specifies the packets that match the access profile are filtered by the switch.	
time_range	Specifies name of this time range entry.	

Restrictions

Only Administrator-level users can issue this command.

Example

To configure an access list entry:

```
DGS-3200-10:4#config access_profile profile_id 101 add access_id 1 ip vlan defau
lt source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit
Command: config access_profile profile_id 101 add access_id 1 ip vlan default so
urce_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit

Success.

DGS-3200-10:4#
```

55-4 show access_profile

Purpose

To display the current access list table.

Format

show access_profile {profile_id <value 1-200>}

Description

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

Parameters

Parameters	Description
profile_id	Specifies the index of the access list profile.

Restrictions

None.

Example

To display the current access list table:

```
DGS-3200-10:4#show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries:199
Total Used Rule Entries  :1


Access Profile ID: 100                                     Type : Ethernet
================================================================================
Owner       : ACL
MASK Option :
VLAN         Source MAC          Destination MAC    802.1P  Ethernet Type
             FF-FF-FF-FF-FF-FF   00-00-00-FF-FF-FF
-----------  -----------------  ----------------- ------  -------------
================================================================================
Unused Entries: 200


Access Profile ID: 101                                     Type : IP
================================================================================
Owner       : ACL
```

```
MASK Option :
VLAN         Source IP MASK  Dst. IP MASK    DSCP ICMP
             255.255.255.255 255.255.255.0
-----------  --------------- --------------- ---- -----------------

Access ID : 1              Mode: Permit                RX Rate(64Kbps): no_limit
Ports     : 1
-----------  --------------- --------------- ---- -----------------
default      20.2.2.3        10.1.1.0        3
================================================================================
Unused Entries: 199

DGS-3200-10:4#
```

55-5 config time_range

Purpose

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

Format

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

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.

Parameters

Parameters	Description
range_name	Specifies the name of the time range settings.
start_time	Specifies the starting time in a day. (24-hr time) For example, 19:00 means 7PM. 19 is also acceptable. **start_time** must be smaller than end_time.
end_time	Specifies the ending time in a day. (24-hr 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)

delete	Deletes 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-level users can issue this command.

Examples

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

```
DGS-3200-10:4#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 wee
kdays mon,fri

Success.

DGS-3200-10:4#
```

55-6 show time_range

Purpose

To display current access list table.

Format

show time_range

Description

This command is used to display current time range settings.

Parameters

None.

Restrictions

None.

Example

To display current time range setting:

```
DGS-3200-10:4#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-3200-10:4#
```

55-7 create cpu access_profile

Purpose

To create CPU access list rules.

Format

create cpu access_profile profile_id <value 1-5>
[ethernet
{ vlan | source_mac <macmask 000000000000-ffffffffffff> |
destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}
| ip
{ vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> |
dscp | [icmp {type | code} | igmp {type } |
tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> |
flag_mask [all | {urg | ack | psh | rst | syn| fin}] } |
udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}
| packet_content_mask
{offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}
| ipv6
{class | flowlabel| source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]

Description

This command is used to create CPU access list rules.

Parameters

Parameters	Description	
vlan	Specifies a VLAN mask.	
source_mac	Specifies the source MAC mask.	
destination_mac	Specifies the destination MAC mask.	
802.1p	Specifies 802.1p priority tag mask.	
ethernet_type	Specifies the Ethernet type mask.	
vlan	Specifies a VLAN mask.	
source_ip_mask	Specifies an IP source submask.	
destination_ip_mask	Specifies an IP destination submask.	
dscp	Specifies the DSCP mask.	
icmp	Specifies that the rule applies to ICMP traffic.	
	type	Specifies the ICMP packet type.
	code	Specifies the ICMP code.
igmp	Specifies that the rule applies to IGMP traffic.	
	type	Specifies the IGMP packet type
tcp	Specifies that the rule applies to TCP traffic.	
	src_port_mask	Specifies the TCP source port mask.
	dst_port_mask	Specifies the TCP destination port mask.
	flag_mask	Specifies the TCP flag field mask.
udp	Specifies that the rule applies to UDP traffic.	
	src_port_mask	Specifies the TCP source port mask.
	dst_port_mask	Specifies the TCP destination port mask.
protocod_id_mask	Specifies that the rule applies to the IP protocol ID traffic.	
	user_define_mask	Specifies the L4 part mask
packet_content_mask	Specifies the packet content mask.	
	offset_0-15	Specifies mask for packet bytes 0-15.
	offset_16-31	Specifies mask for packet bytes 16-31.
	offset_32-47	Specifies mask for packet bytes 32-47.
	offset_48-63	Specifies mask for packet bytes 48-63.
	offset_64-79	Specifies mask for packet bytes 64-79.
class	Specifies the IPv6 class mask.	
flowlabel	Specifies the IPv6 flow label mask.	
source_ipv6_mask	Specifies the IPv6 source IP mask.	

destination_ipv6_mask	Specifies the IPv6 destination IP mask.

Restrictions

Only Administrator-level users can issue this command. The Switch supports a maximum of five CPU profiles to be configured.

Example

To create CPU access list rules:

```
DGS-3200-10:4#create cpu access_profile profile_id 1 ethernet vlan
Command: create cpu access_profile profile_id 1 ethernet vlan

Success.

DGS-3200-10:4#create cpu access_profile profile_id 2 ip source_ip_mask 255.255.2
55.255
Command: create cpu access_profile profile_id 2 ip source_ip_mask 255.255.255.25
5

Success.

DGS-3200-10:4#
```

55-8 delete cpu access_profile

Purpose

To delete CPU access list rules.

Format

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

Description

This command is used to delete CPU access list rules.

Parameters

Parameters	Description
profile_id	Specifies the index of access list profile.
all	Specifies the whole access list profile to delete.

Restrictions

Only Administrator-level users can issue this command. The Switch supports a maximum of 500 access entries. This command can only delete the profile which is created by the CPU ACL module.

Example

To delete access list rules:

```
DGS-3200-10:4#delete cpu access_profile profile_id 3
Command: delete cpu access_profile profile_id 3


Success.


DGS-3200-10:4#
```

55-9 config cpu access_profile

Purpose

To configure a CPU access list entry.

Format

config cpu access_profile profile_id <value 1-5>"

[add access_id <value 1-100>"

[ethernet

{vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |

destination_mac <macaddr 000000000000-ffffffffffff> |

802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> }

| ip

{vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> |

[icmp {type <value 0-255> | code <value 0-255>} |

igmp {type <value 0-255>} |

tcp{src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin } |

udp {src_port <value 0-65535> | dst_port <value 0-65535>} |

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>]

Description

This command is used to configure CPU access list entries.

Parameters

Parameters	Description		
profile_id	Specifies the index of CPU access list profile.		
access_id	Specifies the index of an access list entry. The range of this value is 1 to 100.		
	vlan	Specifies a VLAN name.	
	source_mac	Specifies the source MAC.	
	destination_mac	Specifies the destination MAC.	
	802.1p	Specifies the value of 802.1p priority tag, the value can be configured between 1 and 7.	
	ethernet_type	Specifies the Ethernet type.	
	vlan	Spcifies a VLAN name.	
	source_ip	Specifies an IP source address.	
	destination_ip	Specifies an IP destination address.	
	dscp	Specifies the value of DSCP, the value can be configured from 0 to 63.	
	icmp	Specifies that the rule applies to ICMP traffic.	
		type	Specifies the ICMP packet type.
		code	Specifies the ICMP packet code.
	igmp	Specifies that the rule applies to IGMP traffic.	
		type	Specifies the IGMP packet type.
	tcp	**src_port**	Specifies that the rule applies to the range of TCP source ports.
		dst_port	Specifies the range of the TCP destination port range
		flag	Specifies the TCP flag fields.
	udp	**src_port**	Specifies the range of the TCP source port range.
		dst_port	Specifies the range of the TCP destination port mask
	protocod_id	Specifies that the rule applies to the value of IP protocol ID traffic.	
		user_define	Specifies the L4 part value.

	packet_content	**offset_0-15**	Specifies value for packet bytes 0-15.
		offset_16-31	Specifies value for packet bytes 16-31.
		offset_32-47	Specifies value for packet bytes 32-47.
		offset_48-63	Specifies value for packet bytes 48-63.
		offset_64-79	Specifies value for packet bytes 64-79.
	class	Specifies IPv6 class value.	
	flowlabel	Specifies IPv6 flow label value.	
	source_ipv6	Specifies IPv6 source IP value.	
	destination_ipv6	Specifies IPv6 destionation IP value.	
permit	Specifies the packets that match the access profile are permitted by the switch.		
deny	Specifies the packets that match the access profile are filtered by the switch.		
time_range	Specifies name of this time range entry.		

Restrictions

Only Administrator-level users can issue this command.

Example

To configure access list entry:

```
DGS-3200-10:4#config cpu access_profile profile_id 1 add access_id 1 ethernet vl
an default port 1-3 deny
Command: config cpu access_profile profile_id 1 add access_id 1 ethernet vlan de
fault port 1-3 deny

Success.

DGS-3200-10:4#
```

55-10 show cpu access_profile

Purpose

To display the current CPU access list table.

Format

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

Description

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

Parameters

Parameters	Description
profile_id	Specifies the index of an access list profile.

Restrictions

None.

Example

To display the current CPU access list table:

```
DGS-3200-10:4#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Total Unused Rule Entries:499
Total Used Rule Entries  :1


Access Profile ID: 1                                       Type : Ethernet
================================================================================
MASK Option :
VLAN
-----------

Access ID : 1              Mode: Deny
Ports     : 1-3
-----------
default
================================================================================
Unused Entries: 99
```

```
Access Profile ID: 2                                          Type : IP
================================================================================
MASK Option :
Source IP MASK
255.255.255.255
---------------
================================================================================
Unused Entries: 100


DGS-3200-10:4#
```

55-11 enable cpu_interface_filtering

Purpose

To enable CPU interface filtering.

Format

enable cpu_interface_filtering

Description

This command is used to enable CPU interface filtering.

Parameters

None.

Restrictions

None.

Example

To enable CPU interface filtering:

```
DGS-3200-10:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DGS-3200-10:4#
```

55-12 disable cpu_interface_filtering

Purpose

To disable CPU interface filtering.

Format

disable cpu_interface_filtering

Description

This command is used to disable CPU interface filtering.

Parameters

None.

Restrictions

None.

Example

To disable CPU interface filtering:

```
DGS-3200-10:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering


Success.


DGS-3200-10:4#
```

XIII. Packet Control

The Packet Control section includes the following chapter: Packet Storm.

56 Packet Storm Command List

config traffic control [<portlist> | all] { broadcast [enable| disable]| multicast [enable| disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 512-1024000>| countdown [<value 0> | value 5-30>] | time_interval <value 5-30 > }
config traffic trap [none|storm_occurred|storm_cleared|both]
show traffic control{ <portlist> }

56-1 config traffic control

Purpose

To configure broadcast/multicast/unicast packet storm control. A software mechanism is provided to monitor the traffic rate in addition to the hardware storm control mechanism. If the traffic rate is too high, this port will be shut down.

Format

config traffic control [<portlist> | all] { broadcast [enable| disable]| multicast [enable| disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 512-1024000>| countdown [<value 0> | <value 5-30>] | time_interval <value 5-30 > }

Description

This command is used to configure broadcast/multicast/unicast storm control. Broadcast storm control commands provides H/W storm control mechanism only, and these packet storm control commands include H/W and S/W mechanisms to provide shutdown, recovery, and trap notification functions.

Parameters

Parameters	Description
portlist	Used to specify a range of ports to be configured.
broadcast	Enable or disable broadcast storm control.
multicast	Enable or disable multicast storm control.
unicast	Enable or disable unknown unicast packet storm control (only support drop action).
action	There are two actions to take for storm control, **shutdown** and **drop**. The former is implemented in S/W, and the latter is implemented in

	H/W. If a user chooses **shutdown**, he needs to configure **threshold**, **countdown**, and **time_interval** as well.
threshold	The upper threshold at which the specified storm control will turn on. The **<value 512-1024000>**is the number of broadcast/multicast packets per second received by the switch that will trigger the storm traffic control measure. Must be an unsigned integer.
countdown	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. 0 is the disable forever state.
time_interval	The sampling interval of received packet counts. The possible value will be 5 to 30 seconds. This parameter is meaningless for dropping packets is selected as action.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure traffic control and state:

```
 DGS-3200-10:4#config traffic control 1-10 broadcast enable action shutdown
threshold 512 time_interval 10
 Command: config traffic control 1-10 broadcast enable action shutdown threshold
512 time_interval 10

 Success.

 DGS-3200-10:4#
```

56-2 config traffic trap

Purpose

To configure a traffic control trap.

Format

config traffic trap [none|storm_occurred|storm_cleared|both]

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.

Parameters

Parameters	Description
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-level users can issue this command.

Examples

```
DGS-3200-10:4#config traffic trap both
Command: config traffic trap both


Success.


DGS-3200-10:4#
```

56-3 show traffic control

Purpose

To display current traffic control settings.

Format

show traffic control{ <portlist> }

Description

This command is used to display current traffic control settings.

Parameters

Parameters	Description
portlist	Used to specify a range of ports to be shown. If no parameter is specified, the system will display all port packet storm control configurations.

Restrictions

None.

Examples

To display the packet storm control setting:

```
DGS-3200-10:4#show traffic control
Command: show traffic control



Traffic Storm Control Trap :[None]


Port Thres  Broadcast Multicast Unicast  Action   Count Time    Shutdown
     hold   Storm     Storm     Storm             down  Interval Forever
---- ----- --------- --------- -------- -------- ----- -------- --------
1    512    Disabled  Disabled  Disabled drop     0     5
2    512    Disabled  Disabled  Disabled drop     0     5
3    512    Disabled  Disabled  Disabled drop     0     5
4    512    Disabled  Disabled  Disabled drop     0     5
5    512    Disabled  Disabled  Disabled drop     0     5
6    512    Disabled  Disabled  Disabled drop     0     5
7    512    Disabled  Disabled  Disabled drop     0     5
8    512    Disabled  Disabled  Disabled drop     0     5
9    512    Disabled  Disabled  Disabled drop     0     5
10   512    Disabled  Disabled  Disabled drop     0     5

DGS-3200-10:4#
```

Appendix A - Technical Specifications

General		
Standards	IEEE 802.3 10BASE-T Ethernet	
	IEEE 802.3u 100BASE-TX Fast Ethernet	
	IEEE 802.3ab 1000BASE-T Gigabit Ethernet	
	IEEE 802.3z 1000BASE-T (SFP “Mini GBIC”)	
	IEEE 802.1D/2004/Spanning Tree (802.1s, 802.1w)	
	IEEE 802.1Q-2005 VLAN	
	IEEE 802.1p Priority Queues	
	IEEE 802.1X Network Access Control	
	IEEE 802.3 Nway auto-negotiation	
	IEEE 802.3ad Link Aggregation Control	
	IEEE 802.3x Full-duplex Flow Control	
	IEEE 802.1u Fast Ethernet	
Protocols	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	--	2000Mbps
Fiber Optic	SFP (Mini GBIC) Support	
	IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver)	
	IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver)	
	IEEE 802.3z 1000BASE-SX (DEM-312GT2 transceiver)	
	IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver)	
	IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver)	
	IEEE 802.3z 100BASE-FX (DEM-210 transceiver)	
	IEEE 802.3z 100BASE-FX (DEM-211 transceiver)	
	WDM Single Mode Transceiver 10km (DEM-330T/R)	
	WDM Single Mode Transceiver 40km (DEM-331T/R)	
Topology	Duplex Ring, Duplex Chain	

Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)

Physical and Environmental	
Internal Power Supply	AC Input: 100 – 240 VAC, 50-60 Hz
Power Consumption	DGS-3200-10: 20.9 Watts (Max.) / DGS-3200-16: 28.9 Watts (Max.)
Operating Temperature	DGS-3200-10: 0 - 40°C / DGS-3200-16: 0 - 50°C
Storage Temperature	-40 - 70°C
Humidity	5 - 95% non-condensing
Dimensions	280mm x 180mm x 43mm
Weight	DGS-3200-10: 1.69kg / DGS-3200-16: 1.86kg
EMI	CE Class A, FCC Class A, VCCI Class A, C-Tick Report
Safety	UL, CB Report

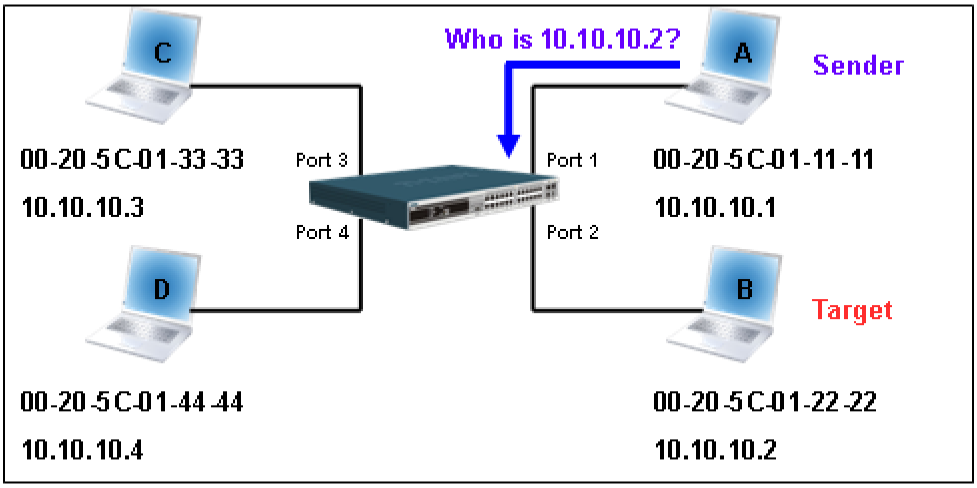
Performance	
Transmission Method	Store-and-forward
Packet Buffer	DGS-3200-10: 128K Byte (1M bit) per device DGS-3200-16: 786K Byte (6M bit) per device
Packet Filtering / Forwarding Rate	Full-wire speed for all connections 1,488,095 pps per port (for 1000Mbps)
MAC Address Learning	Automatic update. DGS-3200-10: Supports 8K MAC address DGS-3200-16: Supports 16K MAC address
Priority Queues	8 Priority Queues per port
Forwarding Table Age Time	Max age: 10-875 seconds, Default = 300

Appendix B - Mitigating ARP Spoofing Attacks Using Packet Content ACL

How Address Resolution Protocol works

In the process of ARP, PC A will first issue an ARP request to query PC B's MAC address. The network structure is shown in Figure 1.

Figure 1



In the meantime, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in the ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00," while PC B's IP address will be written into the "Target Protocol Address," shown in Table 1.

Table 1. ARP Payload

H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
				ARP request	***00-20-5C-01-11-11***	***10.10.10.1***	***00-00-00-00-00-00***	***10.10.10.2***

The ARP request will be encapsulated into an Ethernet frame and sent out. As can be seen in Table 2, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since an ARP request is sent via broadcast, the "Destination address" is in a format of Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Table 2. Ethernet Frame Format

Destination Address	Source Address	Ether-Type	ARP	FCS
FF-FF-FF-FF-FF-FF	***00-20-5C-01-11-11***			

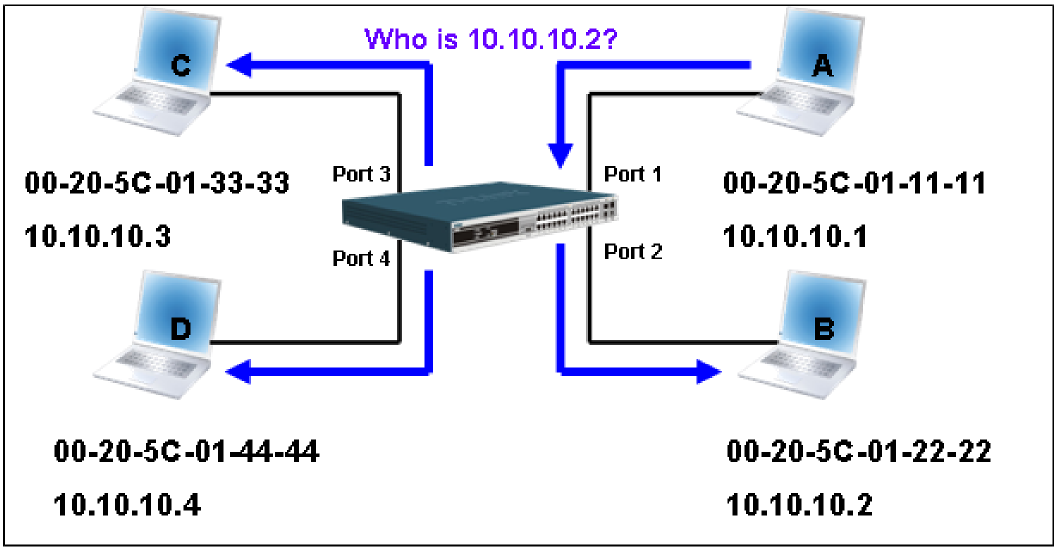
When the switch receives the frame, it will check the "Source Address" in the Ethernet frame's header. If the address is not in its Forwarding Table, the switch will learn PC A's MAC and the associated port into its Forwarding Table.

Port1	00-20-5C-01-11-11

In addition, when the switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure 2).

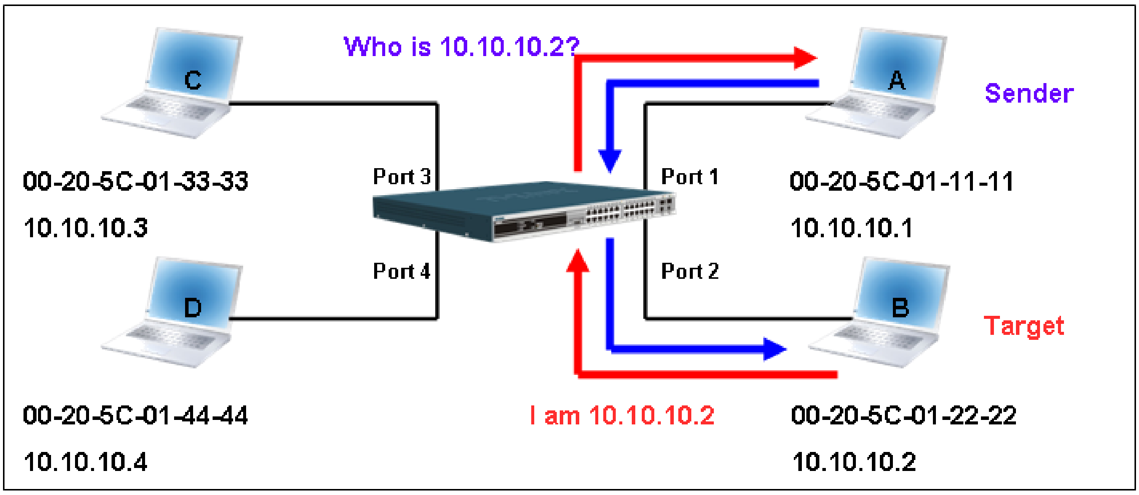
Figure 2

Who is 10.10.10.2?



When the switch floods the frame of ARP request to the network, all PCs will receive and examine the frame but only PC B will reply the query as the destination IP matched (see Figure 3).

Figure 3



When PC B replies to the ARP request, its MAC address will be written into "Target H/W Address" in the ARP payload shown in Table 3. The ARP reply will be then encapsulated into an Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

Table 3. ARP Payload

H/W Type	**Protocol Type**	**H/W Address Length**	**Protocol Address Length**	**Operation**	**Sender H/W Address**	**Sender Protocol Address**	**Target H/W Address**	**Target Protocol Address**
				ARP reply	***00-20-5C-01-11-11***	***10.10.10.1***	***00-20-5C-01-22-22***	***10.10.10.2***

When PC B replies to the query, the "Destination Address" in the Ethernet frame will be changed to PC A's MAC address. The "Source Address" will be changed to PC B's MAC address (see Table 4).

Table 4. Ethernet Frame Format

Destination Address	**Source Address**	**Ether-Type**	**ARP**	**FCS**
00-20-5C-01-11-11	***00-20-5C-01-22-22***			

The switch will also examine the "Source Address" of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B's MAC and update its Forwarding Table.

Forwarding Table

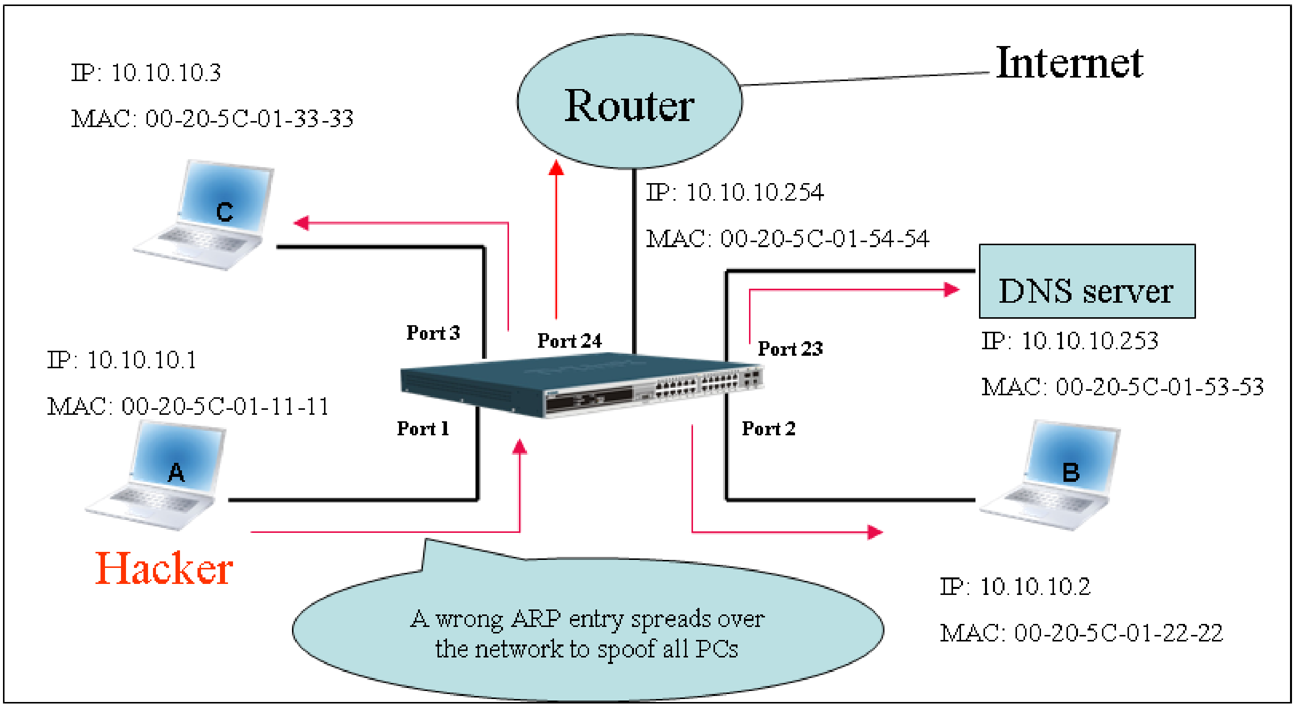
Port1	**00-20-5C-01-11-11**
Port2	**00-20-5C-01-22-22**

How ARP Spoofing Attacks a Network

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service – DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure 4 shows a hacker within a LAN to initiate ARP spoofing attack.

Figure 4



In the Gratuitous ARP packet, the "Sender protocol address" and "Target protocol address" are filled with the same source IP address itself. The "Sender H/W Address" and "Target H/W address" are filled with the same source MAC address itself. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender's MAC and IP address. The format of Gratuitous ARP is shown in the following table.

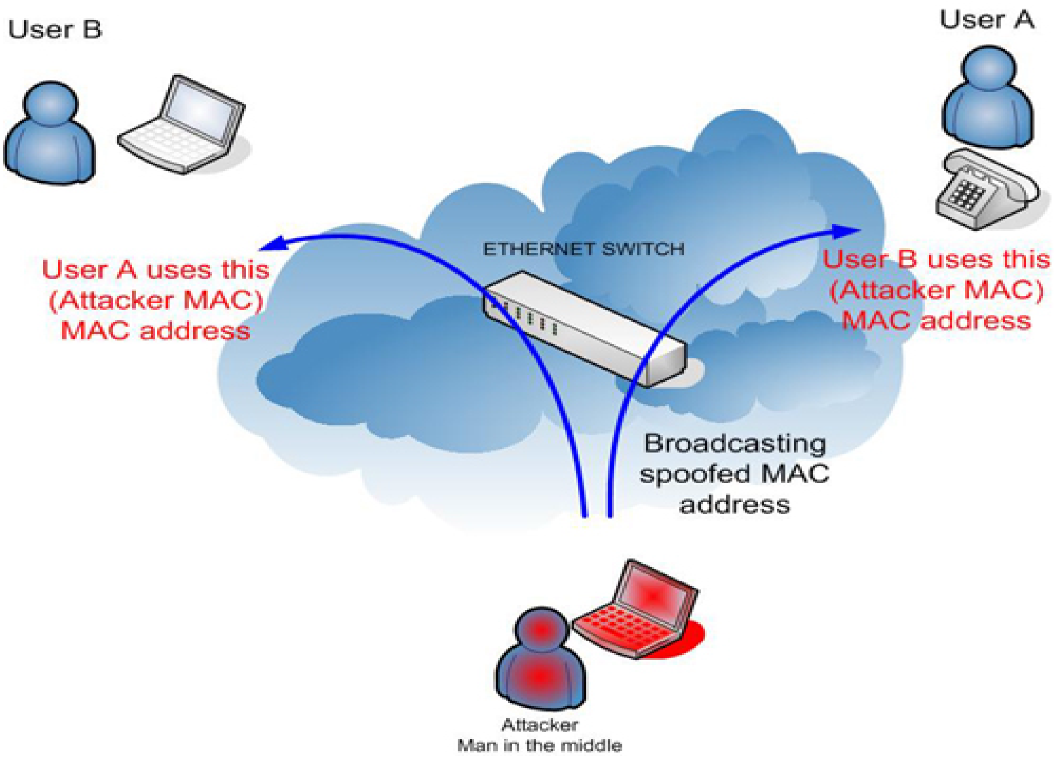
Table 5

Ethernet Header			Gratuitous ARP								
Destination Address	Source Address	Ethernet Type	H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	0806					ARP relay	00-20-5C-01-11-11	10.10.10.254	00-20-5C-01-11-11	10.10.10.254

A common DoS attack today can be done by associating a nonexistent or any specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast one Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker cheats the victim PC that it is a router and cheats the router that it is the victim. As can be seen in Figure 5 all traffic will be then sniffed by the hacker but the users will not discover.

Figure 5

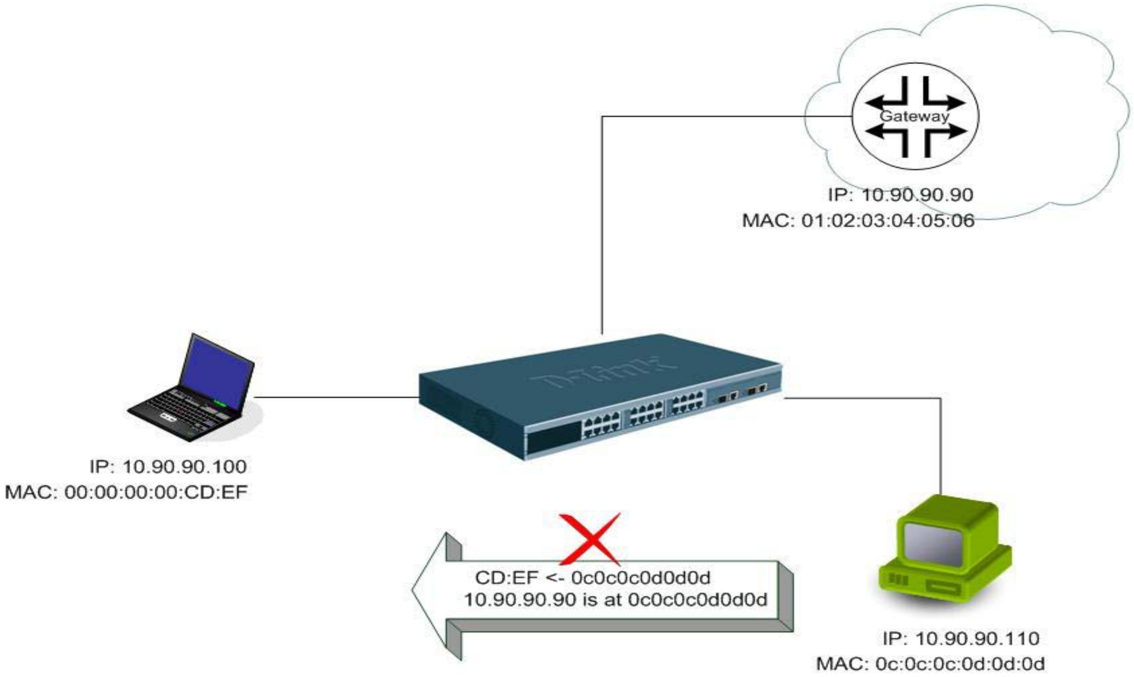


Prevent ARP Spoofing via Packet Content ACL

D-Link managed switches can effectively mitigate common DoS attacks caused by ARP spoofing via a unique Package Content ACL.

For the reason that basic ACL can only filter ARP packets based on packet type, VLAN ID, Source, and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here via using Packet Content ACL to block the invalid ARP packets which contain faked gateway's MAC and IP binding.

Example topology



Configuration

The configuration logic is as follows:

1. Only if the ARP matches Source MAC address in Ethernet, Sender MAC address and Sender IP address in ARP protocol can pass through the switch. (In this example, it is gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL enables users to inspect any offset_chunk. An offset_chunk is a 4-byte block in a HEX format which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of four offset_chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset_chunks can be applied to each profile and a switch. Therefore, a careful consideration is needed for planning and configuration of the valuable offset_chunks.

In Table 6, you will notice that the Offset_Chunk0 starts from the 127th byte and ends at the 128th byte. It also can be found that the offset_chunk is scratched from 1 but not zero.

Table 6. Chunk and Packet Offset

Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset
Chunk	Chunk0	Chunk1	Chunk2	Chunk3	Chunk4	Chunk5	Chunk6	Chunk7	Chunk8	Chunk9	Chunk10	Chunk11	Chunk12	Chunk13	Chunk14	Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset	Offset
Chunk	Chunk16	Chunk17	Chunk18	Chunk19	Chunk20	Chunk21	Chunk22	Chunk23	Chunk24	Chunk25	Chunk26	Chunk27	Chunk28	Chunk29	Chunk30	Chunk31
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

The following table indicates a completed ARP packet contained in Ethernet frame which is the pattern for the calculation of packet offset.

Table 7. A Completed ARP Packet Contained in an Ethernet Frame

Ethernet Header			ARP								
Destination Address	Source Address	Ethernet Type	H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
	01 02 03 04 05 06	0806							0a5a5a5a (10.90.90.90)		

	Command	Description
Step1	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	– Create access profile 1 To match Ethernet Type and Source MAC address.
Step2	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-12 permit	– Configure access profile 1 – Only if the gateway's ARP packet that contains the correct Source MAC in Ethernet frame can pass through the switch.
Step3	create access_profile profile_id 2 profile_name 2 packet_content_mask offset_chunk_1 3 0x0000FFFF Ethernet Type(2-byte) offset_chunk_2 7 0x0000FFFF Sdr IP(First 2-byte) offset_chunk_3 8 0xFFFF0000 Sdr IP(Last 2-byte)	– Create access profile 2 – The first Chunk starts from Chunk 3: mask for Ethernet Type (Blue in Table 6: 13th & 14th bytes) – The second Chunk starts from Chunk 7: mask for Sender IP (First 2-byte) in ARP packet (Green in Table-6: 29th & 30th bytes) – The third Chunk starts from Chunk 8: mask for Sender IP (Last 2-byte) in ARP packet (Brown in Table-6: 31st & 32nd bytes)
Step4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 Ethernet Type(2-byte): ARP offset_chunk_2 0x00000A5A Sdr IP(First 2-byte): 10.90 offset_chunk_3 0x5A5A0000 Sdr IP(Last 2-byte): 90.90 port 1-12 deny	– Configure access profile 2 – The rest the ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step5	Save	– Save config

Appendix C - Password Recovery Procedure

This chapter describes the procedure for resetting passwords on D-Link Switches. Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This chapter explains how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.

2. Power on the Switch. After the runtime image is 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.

```
Boot Procedure                                                   V1.00.B06
-----------------------------------------------------------------------------


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


  MAC Address   : 00-19-5B-EC-32-15
  H/W Version   : A1


  Please wait, loading V1.35.B019 Runtime image.............  00 %

The switch is now entering Password Recovery Mode:_
```

```
The switch is currently in Password Recovery Mode.
>
```

3. In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
reset config	The **reset config** command resets the whole configuration back to the default values.
reboot	The **reboot** command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The **reset** account command deletes all the previously created accounts.
reset password {<username>}	The **reset password** command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The **show account** command displays all previously created accounts.