D-Link®
Building Networks for People

xSTACK®

CLI Reference Guide

Product Model: xStack® DES-3200 Series
Layer 2 Managed Fast Ethernet Switch
Release 4.03

Table of Contents

Chapter 1 Using Command Line Interface

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

This manual provides a reference for all of the commands contained in the CLI. Every command will be introduced in terms of purpose, format, description, parameters, and examples. Configuration and management of the Switch via the Web-based management agent are discussed in the Web UI Reference Guide. For detailed information on installing hardware please also refer to the Hardware Installation Guide.

1-1 Accessing the Switch via the Serial Port

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

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

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

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

```
                        DES-3200-28P Fast Ethernet Switch
                              Command Line Interface

                             Firmware: Build 4.03.004
           Copyright(C) 2012 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DES-3200-28P:admin#
```

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-3200-28P:admin#**. This is the command line where all commands are input.

1-2 Setting the Switch's IP Address

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

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

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

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

  MAC Address   : 00-01-02-03-04-00
  H/W Version   : C1

  Please Wait, Loading 4.03.004 Runtime Image ..............  100 %
  UART init ................................................  100 %
  Starting runtime image
  Device Discovery .........................................  100 %
  Configuration init .......................................      |
```

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

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

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

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

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

```
DES-3200-28P:admin#config ipif System ipaddress 10.24.22.100/255.0.0.0
Command: config ipif System ipaddress 10.24.22.100/8

Success.

DES-3200-28P:admin#
```

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

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

```
..
?
cable_diag ports
cd
cfm linktrace
cfm loopback
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear cfm pkt_cnt
clear counters
clear ethernet_oam ports
clear fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear log
clear mac_based_access_control auth_state
clear mld_snooping data_driven_group
clear mld_snooping statistics counter
clear port_security_entry
config 802.1p default_priority
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.

```
DES-3200-28P:admin#config account
Command: config account
Next possible completions:
<username>

DES-3200-28P:admin#
```

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

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

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

```
DES-3200-28P:admin#config account
Command: config account
Next possible completions:
<username>

DES-3200-28P:admin#config account
```

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

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

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

```
DES-3200-28P:admin#the
Available commands:
..                  ?                   cable_diag          cd
cfm                 clear               config              copy
create              debug               del                 delete
dir                 disable             download            enable
erase               login               logout              md
move                no                  ping                ping6
rd                  reboot              reconfig            rename
reset               save                show                smtp
telnet              traceroute          traceroute6         upload

DES-3200-28P:admin#
```

The top-level commands consist of commands such as **show** or **config**. Most of these commands require one or more parameters to narrow the top-level command. This is equivalent to **show** what? or **config** what? Where the what? is the next parameter.

For example, entering the **show** command with no additional parameters, the CLI will then display all of the possible next parameters.

```
DES-3200-28P:admin#show
Command: show
Next possible completions:
802.1p              802.1x              access_profile      account
accounting          acct_client         address_binding
arp_spoofing_prevention                 arpentry            attack_log
auth_client         auth_diagnostics    auth_session_statistics
auth_statistics     authen              authen_enable       authen_login
authen_policy       authentication      authorization       autoconfig
bandwidth_control   boot_file           bpdu_protection     cfm
command             command_history     config              cpu
cpu_filter          current_config      ddm                 device_status
dhcp_local_relay    dhcp_relay          dos_prevention
dot1v_protocol_group                    dscp                duld
environment         erps                error               ethernet_oam
fdb                 filter              flow_meter          gratuitous_arp
greeting_message    gvrp                igmp                igmp_snooping
ipif                ipif_ipv6_link_local_auto               iproute
ipv6                ipv6route           jumbo_frame         l2protocol_tunnel
lacp_port           limited_multicast_addr                  link_aggregation
lldp                log                 log_save_timing
log_software_module                     loopdetect
mac_based_access_control                mac_based_access_control_local
mac_based_vlan      mac_notification    max_mcast_group
mcast_filter_profile                    mirror              mld_snooping
multicast           multicast_fdb       nlb                 packet
password_recovery   per_queue           poe                 port
port_security       port_security_entry                     port_vlan
ports               power_saving        pppoe               pvid
qinq                radius              rmon                router_ports
safeguard_engine    scheduling          scheduling_mechanism
serial_port         session             sim                 smtp
snmp                sntp                ssh                 ssl
storage_media_info                      stp                 switch
syslog              system_severity     tech_support        terminal
tftp                time                time_range          traffic
traffic_segmentation                    trap                trusted_host
utilization         vlan                vlan_translation    vlan_trunk

DES-3200-28P:admin#
```

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

1-3 Command Syntax Symbols

Syntax	Description
angle brackets < >	Encloses a variable or value. Users must specify the variable or value. For example, in the syntax

	create ipif **<ipif_name 12>** {**<network_address>**} **<vlan_name 32>** {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}} users must supply an IP interface name for **<ipif_name 12>** ,a VLAN name for **<vlan_name 32>** and an address for **<network_address>** when entering the command. DO NOT TYPE THE ANGLE BRACKETS.
square brackets [ ]	Encloses a required value or list of required arguments. Only one value or argument must be specified. For example, in the syntax create account **[admin | operator | power_user | user]** <username 15> {encrypt [plain_text | sha_1] <password>} users 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 create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {**secondary | state** [**enable | disable**] **| proxy_arp** [**enable | disable**] {**local** [**enable | disable**]}} users must specify either the community or trap receiver in the command. DO NOT TYPE THE VERTICAL BAR.
braces { }	Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax reset **{[config | system]} {force_agree}** users may choose configure or system in the command. DO NOT TYPE THE BRACES.
parentheses ( )	Indicates at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified. For example, in the syntax config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}**(1)** users have the option to specify hops or time or both of them. The "(1)" following the set of braces indicates at least one argument or value within the braces must be specified. DO NOT TYPE THE PARENTHESES.
ipif <ipif_name 12> metric <value 1-31>	**12** means the maximum length of the IP interface name. **1-31** means the legal range of the metric value.

1-4 Line Editing Keys

Keys	Description
Delete	Delete character under cursor and shift remainder of line to left.
Backspace	Delete character to left of cursor and shift remainder of line to left.

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

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

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

Chapter 2 Basic Command List

show session
show serial_port
config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}
enable clipaging
disable clipaging
login
logout
?
clear
show command_history
config command_history <value 1-40>
config greeting_message {default}
show greeting_message
config command_prompt [<string 16> | username | default]
config terminal width [default | <value 80-200>]
show terminal width
config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description]}
show ports {<portlist>} {[description | err_disabled | details | media_type]}

2-1 show session

Description

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

Format

show session

Parameters

None.

Restrictions

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

Example

To display the session entries:

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

Total Entries: 2




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

2-2 show serial_port

Description

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

Format

show serial_port

Parameters

None.

Restrictions

None.

Example

To display the serial port setting:

```
DES-3200-28P:admin#show serial_port
Command: show serial_port

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

DES-3200-28P:admin#
```

2-3 config serial_port

Description

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

Format

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

Parameters

baud_rate - (Optional) The serial bit rate that will be used to communicate with the management host. The default baud rate is 115200. **9600** - Specify the serial bit rate to be 9600. **19200** - Specify the serial bit rate to be 19200. **38400** - Specify the serial bit rate to be 38400. **115200** - Specify the serial bit rate to be 115200.
auto_logout - (Optional) The auto logout time out setting. **never** - Never timeout. **2_minutes** - When idle over 2 minutes, the device will auto logout. **5_minutes** - When idle over 5 minutes, the device will auto logout. **10_minutes** - When idle over 10 minutes, the device will auto logout. **15_minutes** - When idle over 15 minutes, the device will auto logout.

Restrictions

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

Example

To configure baud rate:

```
DES-3200-28P:admin#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DES-3200-28P:admin#
```

2-4 enable clipaging

Description

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

Format

enable clipaging

Parameters

None.

Restrictions

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

Example

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

```
DES-3200-28P:admin#enable clipaging
Command: enable clipaging

Success.

DES-3200-28P:admin#
```

2-5 disable clipaging

Description

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

Format

disable clipaging

Parameters

None.

Restrictions

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

Example

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

```
DES-3200-28P:admin#disable clipaging
Command: disable clipaging

Success.

DES-3200-28P:admin#
```

2-6 login

Description

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

Format

login

Parameters

None.

Restrictions

None.

Example

To login the Switch with a user name dlink:

```
DES-3200-28P:admin#login
Command: login

UserName:dlink
PassWord:****

DES-3200-28P:admin#
```

2-7 logout

Description

This command is used to logout the facility.

Format

logout

Parameters

None.

Restrictions

None.

Example

To logout current user:

```
DES-3200-28P:admin#logout
Command: logout


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

                        DES-3200-28P Fast Ethernet Switch
                              Command Line Interface

                             Firmware: Build 4.03.004
           Copyright(C) 2012 D-Link Corporation. All rights reserved.
UserName:
```

2-8 ?

Description

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

Format

?

Parameters

None.

Restrictions

None.

Example

To get “ping” command usage, descriptions:

```
DES-3200-28P:admin#? ping
Command: ? ping

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

DES-3200-28P:admin#
```

2-9 clear

Description

The command is used to clear screen.

Format

clear

Parameters

None.

Restrictions

None.

Example

To clear screen:

```
DES-3200-28P:admin#clear
Command: clear



DES-3200-28P:admin#
```

2-10 show command_history

Description

The command is used to display command history.

Format

show command_history

Parameters

None.

Restrictions

None.

Example

To display command history:

```
DES-3200-28P:admin#show command_history
Command: show command_history

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

DES-3200-28P:admin#
```

2-11 config command_history

Description

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

Format

config command_history <value 1-40>

Parameters

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

Restrictions

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

Example

To configure the number of command history:

```
DES-3200-28P:admin#config command_history 25
Command: config command_history 25

Success.

DES-3200-28P:admin#
```

2-12 config greeting_message

Description

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

Format

config greeting_message {default}

Parameters

default - (Optional) Adding this parameter to the “config greeting_message” command will return the greeting message (banner) to its original factory default entry.

Restrictions

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

Example

To edit the banner:

```
DES-3200-28P:admin#config greeting_message
Command: config greeting_message

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

                   DES-3200-28P Fast Ethernet Switch
                           Command Line Interface

                          Firmware: Build 4.03.004
          Copyright(C) 2012 D-Link Corporation. All rights reserved.
================================================================================

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

2-13 show greeting_message

Description

The command is used to display greeting message.

Format

show greeting_message

Parameters

None.

Restrictions

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

Example

To display greeting message:

```
DES-3200-28P:admin#show greeting_message
Command: show greeting_message

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

                        DES-3200-28P Fast Ethernet Switch
                             Command Line Interface

                            Firmware: Build 4.03.004
          Copyright(C) 2012 D-Link Corporation. All rights reserved.
================================================================================

DES-3200-28P:admin#
```

2-14 config command_prompt

Description

This command is used to modify the command prompt.

The current command prompt consists of four parts: “product name” + “:” + ”user level” + ”#” (e.g. “DES-3200-28P:admin#”). This command is used to modify the first part (1. “product name”) with a string consisting of a maximum of 16 characters, or to be replaced with the users’ login user name.

When users issue the “reset” command, the current command prompt will remain in tact. Yet, issuing the “reset system” will return the command prompt to its original factory default value.

Format

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

Parameters

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

Restrictions

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

Example

To edit the command prompt:

```
DES-3200-28P:admin#config command_prompt Prompt#
Command: config command_prompt Prompt#

Success.

Prompt#:admin#
```

2-15 config terminal width

Description

The command is used to set current terminal width.

The usage is described as below:

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

Format

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

Parameters

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

Restrictions

None.

Example

To configure the current terminal width:

```
DES-3200-28P:admin#config terminal width 120
Command: config terminal width 120

Success.

DES-3200-28P:admin#
```

2-16 show terminal width

Description

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

Format

show terminal width

Parameters

None.

Restrictions

None.

Example

To display the configuration of current terminal width:

```
DES-3200-28P:admin#show terminal width
Command: show terminal width

Global terminal width     : 80
Current terminal width    : 80

DES-3200-28P:admin#
```

2-17 config ports

Description

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

Format

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

Parameters

<portlist> - Enter a list of ports used here.
all - Specify that all the ports will be used for this configuration.
medium_type - (Optional) Specify the medium type while the configure ports are combo ports **fiber** - Specify that the medium type will be set to fiber. **copper** - Specify that the medium type will be set to copper.
speed - (Optional) Specify the port speed of 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 set port speed to 1000_full. While set 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. **master** - Specify that the port(s) will be set to master. **slave** - Specify that the port(s) will be set to slave.
flow_control - (Optional) You can turn on or turn off flow control on one or more ports. By set flow_control to enable or disable. **enable** - Specify that the flow control option will be enabled. **disable** - Specify that the flow control option will be disabled.
learning - (Optional) You can turn on or turn off MAC address learning on one or more ports. **enable** - Specify that the learning option will be enabled. **disable** - Specify that the learning option will be disabled.
state - (Optional) Enables or disables the specified port. If the specificed ports are in error-disabled status , configure their state to enable will recover these ports from disabled to enable state. **enable** - Specify that the port state will be enabled. **disable** - Specify that the port state will be disabled.
mdix - (Optional) MDIX mode can be specified as auto, normal, and cross. If set to normal state, the port is in MDIX mode and can be connected to PC NIC using a straight cale. If set to cross state, the port is in mdi mode, and can be connected to a port (in mdix mode) on another switch thru a straight cabe. **auto** - Specify that the MDIX mode for the port will be set to auto. **normal** - Specify that the MDIX mode for the port will be set to normal. **cross** - Specify that the MDIX mode for the port will be set to cross.
description - (Optional) Specify the description of the port interface. **<desc 1-32>** - Enter the port interface description here. This value can be up to 32 characters long.
clear_description - (Optional) Specify that the description field will be cleared.

Restrictions

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

Example

To configure the ports:

```
DES-3200-28P:admin#config ports all medium_type copper speed auto
Command: config ports all medium_type copper speed auto

Success.

DES-3200-28P:admin#
```

2-18 show ports

Description

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

Format

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

Parameters

ports - Specify a range of ports to be displayed.

<portlist> - (Optional) Enter the list of ports to be configured here.
description - (Optional) Indicates if port description will be included in the display .
err_disabled - (Optional) Indicates if ports are disabled by some reasons will be displayed.
details - (Optional) Displays the port details.
media_type - (Optional) Displays port transceiver type.

Restrictions

None.

Example

To display the port details:

```
DES-3200-28P:admin#show ports details
Command: show ports details

Port : 1
--------------------
Port Status                 : Link Up
Description                 :
HardWare Type               : Fast Ethernet
MAC Address                 : 00-01-02-03-04-01
Bandwidth                   : 100000Kbit
Auto-Negotiation            : Enabled
Duplex Mode                 : Full Duplex
Flow Control                : Disabled
MDI                         : Normal
Address Learning            : Enabled
Last Clear of Counter       : 2 hours 43 mins ago
BPDU Hardware Filtering Mode: Disabled
Queuing Strategy            : FIFO
TX Load                     :   0/100,          0 bits/sec,        0 packets/sec
RX Load                     :   0/100,          0 bits/sec,        0 packets/sec


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

Chapter 3 802.1Q VLAN Command List

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

3-1 create vlan

Description

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

Format

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

Parameters

vlan - The name of the VLAN to be created. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
tag - The VLAN ID of the VLAN to be created. **<vlanid 2-4094>** - Enter the VLAN ID here. The VLAN ID value must be between 2 and 4094.
type 1q_vlan advertisement - (Optional) Specify the VLAN type used is based on the 802.1Q standard and being able to be advertised out.

Restrictions

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

Example

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

```
DES-3200-28P:admin#create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

DES-3200-28P:admin#
```

3-2 create vlan vlanid

Description

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

Format

create vlan vlanid <vidlist> {advertisement}

Parameters

vlanid - The VLAN ID list to be created. **<vidlist>** - Enter the VLAN ID list here.
advertisement - (Optional) Specify the VLAN as being able to be advertised out.

Restrictions

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

Example

To create some VLANs using VLAN ID:

```
DES-3200-28P:admin#create vlan vlanid 10-30
Command: create vlan vlanid 10-30

Success.

DES-3200-28P:admin#
```

3-3 delete vlan

Description

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

Format

delete vlan <vlan_name 32>

Parameters

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

Restrictions

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

Example

To remove a vlan v1:

```
DES-3200-28P:admin#delete vlan v1
Command: delete vlan v1

Success.

DES-3200-28P:admin#
```

3-4 delete vlan vlanid

Description

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

Format

delete vlan vlanid <vidlist>

Parameters

vlanid - The VLAN ID list to be deleted. **<vidlist>** - Enter the VLAN ID list here.

Restrictions

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

Example

To remove VLANs from 10-30:

```
DES-3200-28P:admin#delete vlan vlanid 10-30
Command: delete vlan vlanid 10-30

Success.

DES-3200-28P:admin#
```

3-5 config vlan

Description

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

Format

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

Parameters

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

Restrictions

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

Example

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

```
DES-3200-28P:admin#config vlan v2 add tagged 4-8
Command: config vlan v2 add tagged 4-8

Success.

DES-3200-28P:admin#
```

3-6 config vlan vlanid

Description

This command allows you to configure multiple VLANs at one time. But conflicts will be generated if you configure the name of multiple VLANs at one time.

Format

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

Parameters

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

Restrictions

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

Example

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

```
DES-3200-28P:admin#config vlan vlanid 10-20 add tagged 4-8
Command: config vlan vlanid 10-20 add tagged 4-8

Success.

DES-3200-28P:admin#
```

3-7 config port_vlan

Description

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

Format

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

Parameters

<portlist> - A range of ports for which you want ingress checking. The port list is specified by listing the beginning port number on the Switch, separated by a colon. Then highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. **all** - Specify all ports for ingress checking.
gvrp_state - (Optional) Enabled or disables GVRP for the ports specified in the port list. **enable** - Specify that GVRP for the specified ports will be enabled. **disable** - Specify that GVRP for the specified ports will be disabled.
ingress_checking - (Optional) Enables or disables ingress checking for the specified portlist. **enable** - Specify that ingress checking will be enabled for the specified portlist. **disable** - Specify that ingress checking will be disabled for the specified portlist.

acceptable_frame - (Optional) The type of frame will be accepted by the port. There are two types: **tagged_only** - Only tagged packets can be accepted by this port. **admit_all** - All packets can be accepted.
pvid - (Optional) Specify the PVID of the ports. **<vlanid 1-4094>** - Enter the VLAN ID here. The VLAN ID value must be between 1 and 4094.

Restrictions

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

Example

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

```
DES-3200-28P:admin#config port_vlan 1-5 gvrp_state enable ingress_checking enabl
e acceptable_frame tagged_only pvid 2
Command: config port_vlan 1-5 gvrp_state enable ingress_checking enable acceptab
le_frame tagged_only pvid 2

Success.

DES-3200-28P:admin#
```

3-8 show vlan

Description

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

Format

show vlan {<vlan_name 32>}

Parameters

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

Restrictions

None.

Example

To display VLAN settings:

```
DES-3200-28P:admin#show vlan
Command: show vlan


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


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

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

3-9 show vlan ports

Description

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

Format

show vlan ports {<portlist>}

Parameters

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

Restrictions

None.

Example

To display the VLAN configuration for port 6:

```
DES-3200-28P:admin#show vlan ports 6
Command: show vlan ports 6

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

DES-3200-28P:admin#
```

3-10 show vlan vlanid

Description

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

Format

show vlan vlanid <vidlist>

Parameters

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

Restrictions

None.

Example

To display the VLAN configuration for VLAN ID 1:

```
DES-3200-28P:admin#show vlan vlanid 1
Command: show vlan vlanid 1


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

 Total Entries : 1


DES-3200-28P:admin#
```

3-11 show port_vlan

Description

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

Format

show port_vlan {<portlist>}

Parameters

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

Restrictions

None.

Example

To display 802.1Q port setting:

```
DES-3200-28P:admin#show port_vlan
Command: show port_vlan

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

3-12 enable pvid auto assign

Description

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

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

The default setting is enabled.

Format

enable pvid auto_assign

Parameters

None.

Restrictions

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

Example

To enable the auto-assign PVID:

```
DES-3200-28P:admin#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DES-3200-28P:admin#
```

3-13 disable pvid auto assign

Description

This command is used to disable auto assignment of PVID.

Format

disable pvid auto_assign

Parameters

None.

Restrictions

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

Example

To disable the auto-assign PVID:

```
DES-3200-28P:admin#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DES-3200-28P:admin#
```

3-14 show pvid auto_assign

Description

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

Format

show pvid auto_assign

Parameters

None.

Restrictions

None.

Example

To display PVID auto-assignment state:

```
DES-3200-28P:admin#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DES-3200-28P:admin#
```

3-15 config gvrp

Description

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

Format

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

Parameters

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

Restrictions

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

Example

To set the Join time to 200 milliseconds:

```
DES-3200-28P:admin#config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DES-3200-28P:admin#
```

3-16 show gvrp

Description

This command is used to display the GVRP global setting.

Format

show gvrp

Parameters

None.

Restrictions

None.

Example

To display the global setting of GVRP:

```
DES-3200-28P:admin#show gvrp
Command: show gvrp

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

DES-3200-28P:admin#
```

3-17 enable gvrp

Description

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

Format

enable gvrp

Parameters

None.

Restrictions

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

Example

To enable the generic VLAN Registration Protocol (GVRP):

```
DES-3200-28P:admin#enable gvrp
Command: enable gvrp

Success.

DES-3200-28P:admin#
```

3-18 disable gvrp

Description

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

Format

disable gvrp

Parameters

None.

Restrictions

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

Example

To disable the Generic VLAN Registration Protocol (GVRP):

```
DES-3200-28P:admin#disable gvrp
Command: disable gvrp

Success.

DES-3200-28P:admin#
```

Chapter 4 802.1X Command List

enable 802.1x
disable 802.1x
create 802.1x user <username 15>
delete 802.1x user <username 15>
show 802.1x user
config 802.1x auth_protocol [local | radius_eap]
config 802.1x fwd_pdu system [enable | disable]
config 802.1x fwd_pdu ports [<portlist> | all] [enable | disable]
config 802.1x authorization attributes radius [enable | disable]
show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}
config 802.1x capability ports [<portlist> | all] [authenticator | none]
config 802.1x max_users [<value 1–448> | no_limit]
config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}(1)]
config 802.1x auth_mode [port_based | mac_based]
config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]
config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]
create 802.1x guest_vlan {<vlan_name 32>}
delete 802.1x guest_vlan {<vlan_name 32>}
config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]
show 802.1x guest_vlan
config radius add <server_index 1-3> <server_ip> key <password 32> [default | {auth_port <udp_port_number 1-65535 > | acct_port <udp_port_number 1-65535 > | timeout <sec 1-255> | retransmit <int 1-20>}]
config radius delete <server_index 1-3>
config radius <server_index 1-3> {ipaddress <server_ip> | key <password 32> | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535 > | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}
show radius
show auth_statistics {ports <portlist>}
show auth_diagnostics {ports <portlist>}
show auth_session_statistics {ports <portlist>}
show auth_client
show acct_client
config accounting service [network | shell | system] state [enable | disable]
show accounting service

4-1 enable 802.1x

Description

This command is used to enable the 802.1X function.

Format

enable 802.1x

Parameters

None.

Restrictions

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

Example

Used to enable the 802.1X function:

```
DES-3200-28P:admin#enable 802.1x
Command: enable 802.1x

Success.

DES-3200-28P:admin#
```

4-2 disable 802.1x

Description

This command is used to disable the 802.1X function.

Format

disable 802.1x

Parameters

None.

Restrictions

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

Example

To disable the 802.1X function:

```
DES-3200-28P:admin#disable 802.1x
Command: disable 802.1x

Success.

DES-3200-28P:admin#
```

4-3 create 802.1x user

Description

This command is used to create an 802.1X user.

Format

create 802.1x user <username 15>

Parameters

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

Restrictions

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

Example

To create a 802.1x user “test”:

```
DES-3200-28P:admin#create 802.1x user test
Command: create 802.1x user test

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

DES-3200-28P:admin#
```

4-4 delete 802.1x user

Description

This command is used to delete an 802.1X user.

Format

delete 802.1x user <username 15>

Parameters

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

Restrictions

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

Example

To delete user “test”:

```
DES-3200-28P:admin#delete 802.1x user test
Command: delete 802.1x user test

Success.

DES-3200-28P:admin#
```

4-5 show 802.1x user

Description

This command is used to display the 802.1X user.

Format

show 802.1x user

Parameters

None.

Restrictions

None.

Example

To display the 802.1X user information:

```
DES-3200-28P:admin#show 802.1x user
Command: show 802.1x user

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

 Total Entries:1


DES-3200-28P:admin#
```

4-6 config 802.1x auth_protocol

Description

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

Format

config 802.1x auth_protocol [local | radius_eap]

Parameters

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

Restrictions

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

Example

To configure the 802.1X authentication protocol to RADIUS EAP:

```
DES-3200-28P:admin#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DES-3200-28P:admin#
```

4-7 config 802.1x fwd_pdu system

Description

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

Format

config 802.1x fwd_pdu system [enable | disable]

Parameters

enable - Enable the forwarding of EAPOL PDU.
disable - Disable the forwarding of EAPOL PDU.

Restrictions

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

Example

To configure forwarding of EAPOL PDU system state enable:

```
DES-3200-28P:admin#config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DES-3200-28P:admin#
```

4-8 config 802.1x fwd_pdu ports

Description

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

Format

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

Parameters

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

Restrictions

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

Example

To configure 802.1X fwd_pdu for ports:

```
DES-3200-28P:admin#config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu ports 1-2 enable

Success.

DES-3200-28P:admin#
```

4-9 config 802.1x authorization attributes

Description

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

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

Format

config 802.1x authorization attributes radius [enable | disable]

Parameters

radius - If specified to enable, the authorization attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted. The default state is enabled. **enable** - Specify to enable the authorization attributes. **disable** - Specify to disable the authorization attributes.

Restrictions

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

Example

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

```
DES-3200-28P:admin#config 802.1x authorization attributes radius disable
Command: config 802.1x authorization attributes radius disable

Success.

DES-3200-28P:admin#
```

4-10 show 802.1x

Description

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

Format

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

Parameters

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

Restrictions

None.

Example

To display the 802.1X port level configurations:

```
DES-3200-28P:admin#show 802.1x auth_configuration ports  1
Command: show 802.1x auth_configuration ports 1


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









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

4-11 config 802.1x capability

Description

This command is used to configure the port capability.

Format

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

Parameters

ports - Specify a range of ports to be configured. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specify all ports to be configured.
authenticator - The port that wishes to enforce authentication before allowing access to services that are accessible via that port adopts the authenticator role.
none - Disable authentication on the specified ports.

Restrictions

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

Example

To configure the port capability:

```
DES-3200-28P:admin#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DES-3200-28P:admin#
```

4-12 config 802.1x max_users

Description

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

Format

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

Parameters

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

Restrictions

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

Example

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

```
DES-3200-28P:admin#config 802.1x max_users 200
Command: config 802.1x max_users 200

Success.

DES-3200-28P:admin#
```

4-13 config 802.1x auth_parameter

Description

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

Format

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

Parameters

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

Restrictions

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

Example

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

```
DES-3200-28P:admin#config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

DES-3200-28P:admin#
```

4-14 config 802.1x auth_mode

Description

This command is used to configure 802.1X authentication mode.

Format

config 802.1x auth_mode [port_based | mac_based]

Parameters

port_based - Configure the authentication as port based mode.
mac_based - Configure the authentication as MAC based mode.

Restrictions

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

Example

To configure the authentication mode:

```
DES-3200-28P:admin#config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DES-3200-28P:admin#
```

4-15 config 802.1x init

Description

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

Format

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

Parameters

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

Restrictions

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

Example

To initialize the authentication state machine of some or all:

```
DES-3200-28P:admin#config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-3200-28P:admin#
```

4-16 config 802.1x reauth

Description

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

Format

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

Parameters

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

Restrictions

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

Example

To re-authenticate the device connected to the port:

```
DES-3200-28P:admin#config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DES-3200-28P:admin#
```

4-17 create 802.1x guest_vlan

Description

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

Format

create 802.1x guest_vlan {<vlan_name 32>}

Parameters

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

Restrictions

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

Example

To create a VLAN named "guestVLAN" as 802.1X guest VLAN:

```
DES-3200-28P:admin#create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

DES-3200-28P:admin#
```

4-18 delete 802.1x guest_vlan

Description

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

Format

delete 802.1x guest_vlan {<vlan_name 32>}

Parameters

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

Restrictions

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

Example

To delete the guest VLAN named “guestVLAN”:

```
DES-3200-28P:admin#delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

DES-3200-28P:admin#
```

4-19 config 802.1x guest_vlan

Description

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

Format

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

Parameters

ports - A range of ports enable or disable guest VLAN function. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specify that all the port will be included in this configuration.
state - Specify the guest VLAN port state of the configured ports. **enable** - Specify to join the guest VLAN. **disable** - Specify to be removed from the guest VLAN.

Restrictions

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

Example

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

```
DES-3200-28P:admin#config 802.1x guest_vlan ports 2-8 state enable
Command: config 802.1x guest_vlan ports 2-8 state enable

Warning, The ports are moved to Guest VLAN.

Success.

DES-3200-28P:admin#
```

4-20 show 802.1x guest_vlan

Description

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

Format

show 802.1x guest_vlan

Parameters

None.

Restrictions

None.

Example

To show 802.1X guest VLAN on the Switch:

```
DES-3200-28P:admin#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

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

DES-3200-28P:admin#
```

4-21 config radius add

Description

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

Format

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

Parameters

<server_index 1-3> - Enter the RADIUS server index. This value must be between 1 and 3.
<server_ip> - Enter the IP address of the RADIUS server here.
key - The key pre-negotiated between switch and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over internet. The maximum length of the key is 32. **<password 32>** - Enter the password here. The password can be up to 32 characters long.
default - Sets the authentication UDP port number to 1812 accounting UDP port number to 1813, timeout to 5 seconds and retransmit to 2.
auth_port - (Optional) Specify the UDP port number which is used to transmit RADIUS authentication data between the Switch and the RADIUS server. The range is 1 to 65535. **<udp_port_number 1-65535>** - Enter the authentication port number here. This value must be between 1 and 65535.
acct_port - (Optional) Specify the UDP port number which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. The range is 1 to 65535. **<udp_port_number 1-65535>** - Enter the accounting port number here. This value must be between 1 and 65535.
timeout - (Optional) The time in second for waiting server reply. The default value is 5 seconds. **<sec 1-255>** - Enter the timeout value here. This value must be between 1 and 255 seconds.
retransmit - (Optional) The count for re-transmitting. The default value is 2. **<int 1-20>** - Enter the re-transmit value here. This value must be between 1 and 20.

Restrictions

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

Example

To add a new RADIUS server:

```
DES-3200-28P:admin#config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DES-3200-28P:admin#
```

4-22 config radius delete

Description

This command is used to delete a RADIUS server.

Format

config radius delete <server_index 1-3>

Parameters

<server_index 1-3> - Specify to delete a RADIUS server.Enter the RADIUS server index.

Restrictions

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

Example

To delete a radius server:

```
DES-3200-28P:admin#config radius delete 1
Command: config radius delete 1

Success.

DES-3200-28P:admin#
```

4-23 config radius

Description

This command is used to configure a RADIUS server.

Format

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

Parameters

<server_index 1-3> - Enter the RADIUS server index here. This value must be between 1 and 3.
ipaddress - (Optional) The IP address of the RADIUS server. **<server_ip>** - Enter the RADIUS server IP address here.
key - (Optional) The key pre-negotiated between switch and RADIUS server. It is used to encrypt user's authentication data before being transmitted over internet. The maximum length of the key is 32. **<password 32>** - Enter the key here. The key can be up to 32 characters long.
auth_port - (Optional) Specify the UDP port number which is used to transmit RADIUS authentication data between the Switch and the RADIUS server. The range is 1 to 65535. The default value is 1812. **<udp_port_number 1-65535>** - Enter the authentication port number here. This value must be between 1 and 65535. **default** - Specify that the default port number will be used.
acct_port - (Optional) Specify the UDP port number which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. The range is 1 to 65535. The default value is 1813. **<udp_port_number 1-65535>** - Enter the accounting port number here. This value must be between 1 and 65535. **default** - Specify that the default port number will be used.
timeout - (Optional) The time in second for waiting server reply. The default value is 5 seconds. **<sec 1-255>** - Enter the timeout value here. This value must be between 1 and 255 seconds. **default** - Specify that the default timeout value will be used.

retransmit - (Optional) The count for re-transmitting. The default value is 2.
<int 1-20> - Enter the re-transmit value here. This value must be between 1 and 20.
default - Specify that the default re-transmit value will be used.

Restrictions

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

Example

To configure a radius server:

```
DES-3200-28P:admin#config radius 1 auth_port 60
Command: config radius 1 auth_port 60

Success.

DES-3200-28P:admin#
```

4-24 show radius

Description

This command is used to display RADIUS server configurations.

Format

show radius

Parameters

None.

Restrictions

None.

Example

To display RADIUS server configurations:

```
DES-3200-28P:admin#show radius
Command: show radius

Index  IP Address      Auth-Port Acct-Port Timeout Retransmit Key
                                           (sec)
-----  --------------- --------- --------- ------- ---------- ----------------
1      10.48.74.121    60        1813      5       2          dlink


Total Entries : 1

DES-3200-28P:admin#
```

4-25 show auth_statistics

Description

This command is used to display information of authenticator statistics.

Format

show auth_statistics {ports <portlist>}

Parameters

ports - (Optional) Specify a range of ports to be displayed. **<portlist>** - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator statistics information for port 1:

```
DES-3200-28P:admin#show auth_statistics ports 1
Command: show auth_statistics ports 1


 Port Number : 1

 EapolFramesRx                      0
 EapolFramesTx                      9
 EapolStartFramesRx                 0
 EapolReqIdFramesTx                 6
 EapolLogoffFramesRx                0
 EapolReqFramesTx                   0
 EapolRespIdFramesRx                0
 EapolRespFramesRx                  0
 InvalidEapolFramesRx               0
 EapLengthErrorFramesRx             0

 LastEapolFrameVersion              0
 LastEapolFrameSource               00-00-00-00-00-00




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

4-26 show auth_diagnostics

Description

This command is used to display information of authenticator diagnostics.

Format

show auth_diagnostics {ports <portlist>}

Parameters

ports - (Optional) Specify a range of ports to be displayed. **<portlist>** - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator diagnostics information for port 1:

```
DES-3200-28P:admin#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1


 Port Number : 1

 EntersConnecting                      11
 EapLogoffsWhileConnecting             0
 EntersAuthenticating                  0
 SuccessWhileAuthenticating            0
 TimeoutsWhileAuthenticating           0
 FailWhileAuthenticating               0
 ReauthsWhileAuthenticating            0
 EapStartsWhileAuthenticating          0
 EapLogoffWhileAuthenticating          0
 ReauthsWhileAuthenticated             0
 EapStartsWhileAuthenticated           0
 EapLogoffWhileAuthenticated           0
 BackendResponses                      0
 BackendAccessChallenges               0
 BackendOtherRequestsToSupplicant      0
 BackendNonNakResponsesFromSupplicant  0
 BackendAuthSuccesses                  0
 BackendAuthFails                      0

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

4-27 show auth_session_statistics

Description

This command is used to display information of authenticator session statistics.

Format

show auth_session_statistics {ports <portlist>}

Parameters

ports - (Optional) Specify a range of ports to be displayed. **<portlist>** - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator session statistics information for port 1:

```
DES-3200-28P:admin#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port Number : 1

 SessionOctetsRx                  0
 SessionOctetsTx                  0
 SessionFramesRx                  0
 SessionFramesTx                  0
 SessionId
 SessionAuthenticMethod           Remote Authentication Server
 SessionTime                      0
 SessionTerminateCause            SupplicantLogoff
 SessionUserName

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

4-28 show auth_client

Description

This command is used to display information of RADIUS authentication client.

Format

show auth_client

Parameters

None.

Restrictions

None.

Example

To display authentication client information:

```
DES-3200-28P:admin#show auth_client
Command: show auth_client

radiusAuthClient ==>
 radiusAuthClientInvalidServerAddresses   0
 radiusAuthClientIdentifier

 radiusAuthServerEntry ==>
 radiusAuthServerIndex :1

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

DES-3200-28P:admin#
```

4-29 show acct_client

Description

This command is used to display information of RADIUS accounting client.

Format

show acct_client

Parameters

None.

Restrictions

None.

Example

To display information of RADIUS accounting client:

```
DES-3200-28P:admin#show acct_client
Command: show acct_client

radiusAcctClient ==>
 radiusAcctClientInvalidServerAddresses   0
 radiusAcctClientIdentifier

 radiusAuthServerEntry ==>
 radiusAccServerIndex : 1

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

DES-3200-28P:admin#
```

4-30 config accounting service

Description

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

Format

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

Parameters

network - Accounting service for 802.1X port access control. By default, the service is disabled.
shell - Accounting service for shell events: When user logs on or out the Switch (via the console, Telnet, or SSH) and timeout occurs, accounting information will be collected and sent to RADIUS server. By default, the service is disabled.
system - Accounting service for system events: reset, reboot. By default, the service is disabled.
state - Specify the state of the specified service. **enable** - Specify to enable the specified accounting service. **disable** - Specify to disable the specified accounting service.

Restrictions

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

Example

Enable it to configure accounting shell state:

```
DES-3200-28P:admin#config accounting service shell state enable
Command: config accounting service shell state enable

Success.

DES-3200-28P:admin#
```

4-31 show accounting service

Description

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

Format

show accounting service

Parameters

None.

Restrictions

None.

Example

To show information of RADIUS accounting services:

```
DES-3200-28P:admin#show accounting service
Command: show accounting service

Accounting Service
-------------------
Network      : Enabled
Shell        : Enabled
System       : Enabled

DES-3200-28P:admin#
```

Chapter 5 Access Authentication Control Command List

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

5-1 enable password encryption

Description

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

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

Format

enable password encryption

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the password encryption:

```
DES-3200-28P:admin#enable password encryption
Command: enable password encryption

Success.

DES-3200-28P:admin#
```

5-2 disable password encryption

Description

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

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

Format

disable password encryption

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the password encryption:

```
DES-3200-28P:admin#disable password encryption
Command: disable password encryption

Success.

DES-3200-28P:admin#
```

5-3 enable authen_policy

Description

This command is used to enable system access authentication policy.

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

Format

enable authen_policy

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable system access authentication policy:

```
DES-3200-28P:admin#enable authen_policy
Command: enable authen_policy

Success.

DES-3200-28P:admin#
```

5-4 disable authen_policy

Description

This command is used to disable system access authentication policy.

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

Format

disable authen_policy

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable system access authentication policy:

```
DES-3200-28P:admin#disable authen_policy
Command: disable authen_policy

Success.

DES-3200-28P:admin#
```

5-5 show authen_policy

Description

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

Format

show authen_policy

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display system access authentication policy:

```
DES-3200-28P:admin#show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DES-3200-28P:admin#
```

5-6 create authen_login

Description

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

Format

create authen_login method_list_name <string 15>

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DES-3200-28P:admin#
```

5-7 config authen_login

Description

Configure a user-defined or default method list of authentication methods for user login. The sequence of methods will effect the altercation result. For example, if the sequence is tacacs+ first, then tacacs and local, when user trys to login, the authentication request will be sent to the first server host in tacacs+ built-in server group. If the first server host in tacacs+ group is missing, the authentication request will be sent to the second server host in tacacs+ group, and so on. If all server hosts in tacacs+ group are missing, the authentication request will be sent to the first server host in tacacs group…If all server hosts in tacacs group are missing, the local account database in the device is used to authenticate this user. When user logins the device successfully while using methods like tacacs/xtacacs/tacacs+/radius built-in or user-defined server groups or none, the “user” privilege level is assigned only. If user wants to get admin privilege level, user must use the “enable admin” command to promote his privilege level. But when local method is used, the privilege level will depend on this account privilege level stored in the local device.

Format

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

Parameters

default - The default method list of authentication methods.
method_list_name - The user-defined method list of authentication methods. **<string 15>** - Enter the method list name here. This value can be up to 15 characters long.
method - Specify the authentication method used. **tacacs** - (Optional) Authentication by the built-in server group “tacacs”. **xtacacs** - (Optional) Authentication by the built-in server group “xtacacs”.

tacacs+ - (Optional) Authentication by the built-in server group “tacacs+”.
radius - (Optional) Authentication by the built-in server group “radius”.
server_group - (Optional) Authentication by the user-defined server group.
<string 15> - Enter the server group value here. This value can be up 15 characters long.
local - (Optional) Authentication by local user account database in device.
none - (Optional) No authentication.

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#config authen_login method_list_name login_list_1 method
tacacs+ tacacs local
Command: config authen_login method_list_name login_list_1 method tacacs+
tacacs local

Success.

DES-3200-28P:admin#
```

5-8 delete authen_login

Description

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

Format

delete authen_login method_list_name <string 15>

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DES-3200-28P:admin#
```

5-9 show authen_login

Description

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

Format

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

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#show authen_login method_list_name login_list_1
Command: show authen_login method_list_name login_list_1

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

DES-3200-28P:admin#
```

5-10 create authen_enable

Description

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

Format

create authen_enable method_list_name <string 15>

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

DES-3200-28P:admin#
```

5-11 config authen_enable

Description

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

Format

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

Parameters

default - The default method list of authentication methods.
method_list_name - The user-defined method list of authentication methods. **<string 15>** Enter the method list name here. This value can be up to 15 characters long.
method - Specify the authentication method used. **tacacs** - (Optional) Authentication by the built-in server group "tacacs". **xtacacs** - (Optional) Authentication by the built-in server group "xtacacs". **tacacs+** - (Optional) Authentication by the built-in server group "tacacs+". **radius** - (Optional) Authentication by the built-in server group "radius". **server_group** - (Optional) Authentication by the user-defined server group. **<string 15>** - Enter the server group name here. This value can be up to 15 characters long. **local_enable** - (Optional) Authentication by local enable password in device. **none** - (Optional) No authentication.

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#config authen_enable method_list_name enable_list_1 method
tacacs+ tacacs local_enable
Command: config authen_ enable method_list_name enable_list_1 method tacacs+
tacacs local_enable

Success.

DES-3200-28P:admin#
```

5-12 delete authen_enable

Description

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

Format

delete authen_enable method_list_name <string 15>

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DES-3200-28P:admin#
```

5-13 show authen_enable

Description

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

Format

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

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#show authen_enable method_list_name enable_list_1
Command: show authen_enable method_list_name enable_list_1

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

DES-3200-28P:admin#
```

5-14 config authen application

Description

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

Format

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

Parameters

console - Application: console.
telnet - Application: telnet.
ssh - Application: SSH.
http - Application: web.
all - Application: console, telnet, SSH, and web.
login - 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 - Default method list.
method_list_name - The user-defined method list name. **<string>** - Enter the method list name here. This value can be up to 15 characters long.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the login method list for telnet:

```
DES-3200-28P:admin#config authen application telnet login method_list_name
login_list_1
Command: config authen application telnet login method_list_name login_list_1

Success.

DES-3200-28P:admin#
```

5-15 show authen application

Description

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

Format

show authen application

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#show authen application
Command: show authen application

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

DES-3200-28P:admin#
```

5-16 create authen server_group

Description

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

Format

create authen server_group <string 15>

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

To create a user-defined authentication server group:

```
DES-3200-28P:admin#create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DES-3200-28P:admin#
```

5-17 config authen server_group

Description

This command is used to add or remove an authentication server host to or from the specified server group. Built-in server group “tacacs”, “xtacacs”, “tacacs+”, “radius” accepts the server host with the same protocol only, but user-defined server group can accept server hosts with different protocols.

Format

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

Parameters

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

add - Add a server host to a server group. **delete** - Remove a server host from a server group.
server_host - Server host's IP address. **<ipaddr>** - Enter the server host IP address here.
protocol - Specify the authentication protocol used. **tacacs** - Specify that the TACACS authentication protocol will be used. **xtacacs** - Specify that the XTACACS authentication protocol will be used. **tacacs+** - Specify that the TACACS+ authentication protocol will be used. **radius** - Specify that the radius authentication protocol will be used.

Restrictions

Only Administrator-level users can issue this command.

Example

To add an authentication server host to an server group:

```
DES-3200-28P:admin#config authen server_group mix_1 add server_host 10.1.1.222
protocol
tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol
ta
cacs+

Success.

DES-3200-28P:admin#
```

5-18 delete authen server_group

Description

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

Format

delete authen server_group <string 15>

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a user-defined authentication server group:

```
DES-3200-28P:admin#delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DES-3200-28P:admin#
```

5-19 show authen server_group

Description

This command is used to display the authentication server groups.

Format

show authen server_group {<string 15>}

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

To display all authentication server groups:

```
DES-3200-28P:admin#show authen server_group
Command: show authen server_group

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

Total Entries : 5

DES-3200-28P:admin#
```

5-20 create authen server_host

Description

This command is used to create an authentication server host. When an authentication server host is created, IP address and protocol are the index. That means over 1 authentication protocol

services can be run on the same physical host. The maximum supported number of server hosts is 16.

Format

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

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#create authen server_host 10.1.1.222 protocol tacacs+ port
15555 timeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555
timeout 10

Key is empty for TACACS+ or RADIUS.
Success.

DES-3200-28P:admin#
```

5-21 config authen server_host

Description

This command is used to configure an authentication server host.

Format

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

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#config authen server_host 10.1.1.222 protocol tacacs+ key
"This is a secret."
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a
secret."

Success.

DES-3200-28P:admin#
```

5-22 delete authen server_host

Description

This command is used to delete an authentication server host.

Format

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

Parameters

<ipaddr> - Enter the server host's IP address.
protocol - Specify that server host's authentication protocol. **tacacs** - Server host's authentication protocol. **xtacacs** - Server host's authentication protocol. **tacacs+** - Server host's authentication protocol. **radius** - Server host's authentication protocol.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete an authentication server host:

```
DES-3200-28P:admin#delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

DES-3200-28P:admin#
```

5-23 show authen server_host

Description

This command is used to display the authentication server hosts.

Format

show authen server_host

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display all authentication server hosts:

```
DES-3200-28P:admin#show authen server_host
Command: show authen server_host

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

Total Entries : 1

DES-3200-28P:admin#
```

5-24 config authen parameter response_timeout

Description

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

Format

config authen parameter response_timeout <int 0-255>

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DES-3200-28P:admin#
```

5-25 config authen parameter attempt

Description

This command is used to configure the maximum attempts for user's trying to login or promote the privilege on console, telnet, SSH application.

Format

config authen parameter attempt <int 1-255>

Parameters

<int 1-255> - The amount of attempts for user's trying to login or promote the privilege on console or telnet or SSH. This value must be between 1 and 255. Default value is 3.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the maximum attempts for user's trying to login or promote the privilege to be 9:

```
DES-3200-28P:admin#config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DES-3200-28P:admin#
```

5-26 show authen parameter

Description

This command is used to display the parameters of authentication.

Format

show authen parameter

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the parameters of authentication:

```
DES-3200-28P:admin#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DES-3200-28P:admin#
```

5-27 enable admin

Description

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

This command can not be used when authentication policy is disabled.

Format

enable admin

Parameters

None.

Restrictions

None.

Example

To enable administrator lever privilege:

```
DES-3200-28P:puser#enable admin
Command: enable admin

PassWord:******
Success.

DES-3200-28P:admin#
```

5-28 config admin local_enable

Description

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

Format

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

Parameters

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

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the administrator password:

```
DES-3200-28P:admin#config admin local_enable
Command: config admin local_ebable

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

DES-3200-28P:admin#
```

Chapter 6 Access Control List (ACL) Command List

create access_profile profile_id <value 1-4> profile_name <name 32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip { vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code } | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]
delete access_profile [profile_id <value 1-4> | profile_name <name 32> | all]
config access_profile [profile_id <value 1-4> | profile_name <name 32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type<value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter[enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete access_id <value1-256>]
show access_profile {[profile_id <value 1-4> | profile_name <name 32>]}
config flow_meter [profile_id <value 1-4> | profile_name <name 32>] access_id <value 1-256> [rate [<value 1-1048576>] {burst_size [<value 1-262144>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 1-1048576> {cbs <value 1-262144>} pir <value 1-1048576> {pbs <value 1-262144>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 1-1048576> cbs <value 1-262144> ebs <value 1-262144> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]
show flow_meter {[profile_id <value 1-4> | profile_name <name 32>] {access_id <value 1-256>}}
config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time

hh:mm:ss> weekdays <daylist> | delete]
show time_range
show current_config access_profile

6-1 create access_profile

Description

This command is used to create access control list profiles.

When creating ACL, each profile can have 256 rules/access IDs. However, when creating ACL type as Ethernet or IPv4 at the first time, 62 rules are reserved for the system. In this case, only 194 rules are available to configure. You can use the **show access_prfile** command to see the available rules.

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

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

The Switch supports the following profile types:

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

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

Format

create access_profile profile_id <value 1-4> profile_name <name 32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip { vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code } | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class |

flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]

Parameters

profile_id - Specify the index of the access list profile.
- **<value 1-4>** - Enter the profile ID here. This value must be between 1 and 4.

profile_name - The name of the profile must be specified. The maximum length is 32 characters.
- **<name 32>** - Enter the profile name here.

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

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

packet_content_mask - Specify the packet content mask. Only one packet_content_mask profile can be created.
- **offset_chunk_1** - (Optional) Specify that the offset chunk 1 will be used.

<value 0-31> - Enter the offset chunk 1 value here. This value must be between 0 and 31.
<hex 0x0-0xffffffff> - Enter the offset chunk 1 mask here.
offset_chunk_2 - (Optional) Specify that the offset chunk 2 will be used.
<value 0-31> - Enter the offset chunk 2 value here. This value must be between 0 and 31.
<hex 0x0-0xffffffff> - Enter the offset chunk 2 mask here.
offset_chunk_3 - (Optional) Specify that the offset chunk 3 will be used.
<value 0-31> - Enter the offset chunk 3 value here. This value must be between 0 and 31.
<hex 0x0-0xffffffff> - Enter the offset chunk 3 mask here.
offset_chunk_4 - (Optional) Specify that the offset chunk 4 will be used.
<value 0-31> - Enter the offset chunk 4 value here. This value must be between 0 and 31.
<hex 0x0-0xffffffff> - Enter the offset chunk 4 mask here.

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

Restrictions

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

Example

To create three access profiles:

```
DES-3200-28P:admin#create access_profile profile_id 1 profile_name t1 ethernet
vlan source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p
ethernet_type
Command: create access_profile profile_id 1 profile_name 1 ethernet vlan
source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p
ethernet_type

Success.

DES-3200-28P:admin#create access_profile profile_id 2 profile_name 2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create access_profile profile_id 2 profile_name t2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DES-3200-28P:admin#create access_profile profile_id 4 profile_name 4
packet_content_mask offset_chunk_1 3 0xFFFF offset_chunk_2 5 0xFF00
offset_chunk_3 14 0xFFFF0000 offset_chunk_4 16 0xFF000000
Command: create access_profile profile_id 4 profile_name 4 packet_content_mask
offset_chunk_1 3 0xFFFF offset_chunk_2 5 0xFF00 offset_chunk_3 14 0xFFFF0000
offset_chunk_4 16 0xFF000000

Success.

DES-3200-28P:admin#
```

6-2 delete access_profile

Description

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

Format

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

Parameters

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

Restrictions

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

Example

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

```
DES-3200-28P:admin#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DES-3200-28P:admin#
```

6-3 config access_profile

Description

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

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

Format

config access_profile [profile_id <value 1-4> | profile_name <name 32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type<value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter[enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete access_id <value1-256>]

Parameters

profile_id - Specify the index of the access list profile. **<value 1-4>** - Enter the profile ID value here. This value must be between 1 and 4.
profile_name - Specify the name of the profile. **<name 32>** - Enter the profile name here. This name can be up to 32 characters long.
add - Specify that a profile or a rule will be added.
access_id - Specify the index of the access list entry. The value range is 1-256, but the supported maximum number of entries depends on the project. If the auto_assign option is selected, the access ID is automatically assigned, when adding multiple ports.

auto_assign - Specify that the access ID will automatically be assigned.
<value 1-256> - Enter the access ID used here. This value must be between 1 and 256.

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

ip - Specify to configure the IP access profile.
vlan - (Optional) Specify a VLAN name.
<vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.
vlan_id - (Optional) Specify that VLAN ID used.
<vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.
mask – (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0x0fff> - Enter the mask value here.
source_ip - (Optional) Specify an IP source address.
<ipaddr> - Enter the source IP address used for this configuration here.
mask - (Optional) Specify an additional mask parameter that can be configured.
<netmask> - Enter the source netmask used here.
destination_ip - (Optional) Specify an IP destination address.
<ipaddr> - Enter the destination IP address used for this configuration here.
mask - (Optional) Specify an additional mask parameter that can be configured.
<netmask> - Enter the destination netmask used here.
dscp - (Optional) Specify the value of DSCP. The DSCP value ranges from 0 to 63.
<value 0-63> - Enter the DSCP value here.
icmp - (Optional) Specify to configure the ICMP parameters.
type - (Optional) Specify that the rule will apply to the ICMP Type traffic value.
<value 0-255> - Enter the ICMP type traffic value here. This value must be between 0 and 255.
code - (Optional) Specify that the rule will apply to the ICMP Code traffic value.
<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.
igmp - (Optional) Specify to configure the IGMP parameters.
type - (Optional) Specify that the rule will apply to the IGMP Type traffic value.
<value 0-255> - Enter the IGMP type traffic value here. This value must be between 0 and 255.
tcp - Specify to configure the TCP parameters.
src_port - (Optional) Specify that the rule will apply to a range of TCP source ports.
<value 0-65535> - Enter the TCP source port value here. This value must be between 0 and 65535.
mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the source port mask here.
dst_port - (Optional) Specify that the rule will apply to a range of TCP destination ports.
<value 0-65535> - Enter the TCP destination port value here. This value must be between 0 and 65535.

mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the destination port mask here.
flag - (Optional) Specify the TCP flag fields.
all - Specify that all the TCP flags will be used in this configuration.
urg - (Optional) Specify that the TCP flag field will be set to 'urg'.
ack - (Optional) Specify that the TCP flag field will be set to 'ack'.
psh - (Optional) Specify that the TCP flag field will be set to 'psh'.
rst - (Optional) Specify that the TCP flag field will be set to 'rst'.
syn - (Optional) Specify that the TCP flag field will be set to 'syn'.
fin - (Optional) Specify that the TCP flag field will be set to 'fin'.
udp - Specify to configure the UDP parameters.
src_port - (Optional) Specify the UDP source port range.
<value 0-65535> - Enter the UDP source port value here. This value must be between 0 and 65535.
mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the source port mask here.
dst_port - (Optional) Specify the UDP destination port range.
<value 0-65535> - Enter the UDP destination port value here. This value must be between 0 and 65535.
mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the destination port mask here.
protocol_id - Specify that the rule will apply to the value of IP protocol ID traffic.
<value 0-255> - Enter the protocol ID used here.
user_define - (Optional) Specify that the rule will apply to the IP protocol ID and that the mask options behind the first 4 bytes of the IP payload.
<hex 0x0-0xffffffff> - Enter the user-defined mask value here.
mask - Specify an additional mask parameter that can be configured.
<hex 0x0-0xffffffff> - Enter the mask value here.

packet_content - A maximum of 4 offsets can be specified. Each offset defines 4 bytes of data which is identified as a single UDF field.
offset_chunk_1 – (Optional) Specify the value of the packet bytes to be matched. Offset chunk 1 will be used.
<hex 0x0-0xffffffff> - Enter the offset chunk 1 mask here.
offset_chunk_2 - (Optional) Specify the value of the packet bytes to be matched. Offset chunk 2 will be used.
<hex 0x0-0xffffffff> - Enter the offset chunk 2 mask here.
offset_chunk_3 - (Optional) Specify the value of the packet bytes to be matched. Offset chunk 3 will be used.
<hex 0x0-0xffffffff> - Enter the offset chunk 3 mask here.
offset_chunk_4 - (Optional) Specify the value of the packet bytes to be matched. Offset chunk 4 will be used.
<hex 0x0-0xffffffff> - Enter the offset chunk 4 mask here.

ipv6 - Specify that the rule applies to IPv6 fields.
class - (Optional) Specify the value of the IPv6 class.
<value 0-255> - Enter the IPv6 class value here. This value must be between 0 and 255.
flowlabel - (Optional) Specify the value of the IPv6 flow label.
<hex 0x0-0xffff> - Enter the IPv6 flow label mask used here.
source_ipv6 - (Optional) Specify the value of the IPv6 source address.
<ipv6addr> - Enter the source IPv6 address used for this configuration here.
mask - (Optional) Specify an additional mask parameter that can be configured.
<ipv6mask> - Enter the source IPv6 mask here.
destination_ipv6 - (Optional) Specify the value of the IPv6 destination address.
<ipv6addr> - Enter the destination IPv6 address used for this configuration here.
mask - (Optional) Specify an additional mask parameter that can be configured.
<ipv6mask> - Enter the destination IPv6 mask here.
tcp - (Optional) Specify to configure the TCP parameters.
src_port - Specify the value of the IPv6 Layer 4 TCP source port.
<value 0-65535> - Enter the TCP source port value here. This value must be between 0 and 65535.
mask - Specify an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the TCP source port mask value here.
dst_port - (Optional) Specify the value of the IPv6 Layer 4 TCP destination port.
<value 0-65535> - Enter the TCP destination port value here. This value must be between 0 and 65535.
mask - Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the TCP destination port mask value here.
udp - (Optional) Specify to configure the UDP parameters.
src_port - Specify the value of the IPv6 Layer 4 UDP source port.
<value 0-65535> - Enter the UDP source port value here. This value must be between 0 and 65535.
mask - Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the UDP source port mask value here.
dst_port - Specify the value of the IPv6 Layer 4 UDP destination port.
<value 0-65535> - Enter the UDP destination port value here. This value must be between 0 and 65535.
mask - Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the UDP destination port mask value here.
icmp - (Optional) Specify to configure the ICMP parameters used.
type - (Optional) Specify that the rule applies to the value of ICMP type traffic.
<value 0-255> - Enter the ICMP type traffic value here. This value must be between 0 and 255.
code - (Optional) Specify that the rule applies to the value of ICMP code traffic.
<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.

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

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

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

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

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

delete - Specify that a profile or a rule will be deleted.
access_id - Specify the index of the access list entry. The value range is 1-256, but the supported maximum number of entries depends on the project. **<value 1-256>** - Enter the access ID used here. This value must be between 1 and 256.

Restrictions

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

Example

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

```
DES-3200-28P:admin#config access_profile profile_id 3 add access_id auto_assign
packet_content offset_chunk_3 0xF0 port all deny
Command: config access_profile profile_id 3 add access_id auto_assign
packet_content offset_chunk_3 0xF0 port all deny

Success.

DES-3200-28P:admin#
```

6-4 show access_profile

Description

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

Format

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

Parameters

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

Restrictions

None.

Example

To display the current access list table:

```
DES-3200-28P:admin#show access_profile
Command: show access_profile

Access Profile Table

Total User Set Rule Entries : 4
```

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

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

MASK on
    VLAN            : 0xFFF
    802.1p
    Ethernet Type

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

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

Action:
    Permit

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

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

MASK on
    VLAN            : 0xFFF
    DSCP
    ICMP

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

Match on
    VLAN ID         : 1
    DSCP            : 0

Action:
    Permit

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

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

MASK on
    Class
    TCP
```

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

Match on
    Class           : 0

Action:
    Permit

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

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

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

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

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

Action:
    Permit
    Priority               : 1
    Replace DSCP           : 1

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

DES-3200-28P:admin#
```

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

```
DES-3200-28P:admin#show access_profile profile_id 2
Command: show access_profile profile_id 2

Access Profile Table

Profile ID: 2    Profile Name: 2                      Type : Ethernet
Mask on
    VLAN              : 0xF
    Source MAC       : FF-FF-FF-00-00-00
    Destination MAC : 00-00-00-FF-FF-FF
Available HW Entries: 255
-------------------------------------------------------------------------------
```

```
-
Rule ID : 22       Ports: 1-7
Match on
   VLAN ID           : 8                      Mask : 0xFFF
   Source MAC       : 00-01-02-03-04-05   Mask : FF-FF-FF-FF-FF-FF
   Destination MAC :00-05-04-03-02-00    Mask : FF-FF-FF-FF-FF-00
Action:
Deny

DES-3200-28P:admin#
```

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

```
DES-3200-28P:admin#show access_profile profile_id 4
Command: show access_profile profile_id 4

Access Profile Table


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

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

Available HW Entries : 255
-------------------------------------------------------------------------------
Rule ID : 1       Ports: 1-2

Match on
    offset_chunk_1 : 3      value : 0x000086DD
    offset_chunk_2 : 5      value : 0x00003A00
    offset_chunk_3 : 14     value : 0x86000000

Action:
    Deny

DES-3200-28P:admin#
```

6-5 config flow_meter

Description

This command is used to configure the flow-based metering function. The metering function supports three modes: single rate two color, single rate three color, and two rate three color. The access rule must be created before the parameters of this function can be applied.

For the single rate two color mode, users may set the preferred bandwidth for this rule, in Kbps, and once the bandwidth has been exceeded, overflowing packets will either be dropped or have a drop precedence set, depending on the user configuration.

For single rate three color mode, users need to specify the committed rate, in Kbps, the committed burst size, and the excess burst size.

For the two rate three color mode, users need to specify the committed rate in Kbps, the committed burst size, the peak rate and the peak burst size.

There are two cases for mapping the color of a packet: Color-blind mode and Color-aware mode. In the Color-blind case, the determination for the packet's color is based on the metering result. In the Color-aware case, the determination for the packet's color is based on the metering result and the ingress DSCP.

When color-blind or color-aware is not specified, color-blind is the default mode.

The green color packet will be treated as the conforming action, the yellow color packet will be treated as the exceeding action, and the red color packet will be treated as the violating action.

The replace DSCP action can be performed on packets that conform (GREEN) and packets that do not conform (YELLOW and RED). If drop YELLOW/RED is selected, the action to replace the DSCP will not take effect.

Format

config flow_meter [profile_id <value 1-4> | profile_name <name 32>] access_id <value 1-256> [rate [<value 1-1048576>] {burst_size [<value 1-262144>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 1-1048576> {cbs <value 1-262144>} pir <value 1-1048576> {pbs <value 1-262144>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 1-1048576> cbs <value 1-262144> ebs <value 1-262144> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]

Parameters

profile_id - Specify the profile ID. **<value 1-4>** - Enter the profile ID here. This value must be between 1 and 4.
profile_name - Specify the name of the profile. The maximum length is 32 characters. **<name 32>** - Enter the profile name used here.
access_id - Specify the access ID. **<value 1-256>** - Enter the access ID used here. This value must be between 1 and 256.
rate - This specifies the rate for single rate two color mode. Specify the committed bandwidth in Kbps for the flow. The value m and n are determined by the project. **<value 1-1048576>** - Enter the rate for single rate two color mode here. This value must be between 1 and 1048576.
burst_size - (Optional) This specifies the burst size for the single rate two color mode. The unit is Kbytes. **<value 1-262144>** - Enter the burst size value here. This value must be between 1 and 262144.
rate_exceed - This specifies the action for packets that exceeds the committed rate in single rate, two color mode. **drop_packet** - Drop the packet immediately. **remark_dscp** - Mark the packet with a specified DSCP. The packet is set to have a high drop precedence. **<value 0-63>** - Enter the remark DSCP value here. This value must be between 0 and 63.
tr_tcm - Specify the "two rate three color mode".

cir - Specify the Committed Information Rate. The unit is in Kbps. CIR should always be equal or less than PIR.
<value 1-1048576> - Enter the commited information rate value here. This value must be between 1 and 1048576.
cbs - (Optional) Specify the “Committed Burst Size”. The unit is Kbytes. That is to say, 1 means 1Kbytes. This parameter is an optional parameter. The default value is 4*1024.
<value 1-262144> - Enter the commited burst size value here. This value must be between 1 and 262144.
pir - Specify the “Peak Information Rate”. The unit is in Kbps. PIR should always be equal to or greater than CIR.
<value 1-1048576> - Enter the peak information rate value here. This value must be between 1 and 1048576.
pbs - (Optional) Specify the “Peak Burst Size”. The unit is in Kbytes. This parameter is an optional parameter. The default value is 4*1024.
<value 1-262144> - Enter the peak burst size value here. This value must be between 1 and 262144.
color_blind - (Optional) Specify the meter mode as color-blind. The default is color-blind mode.
color_aware - (Optional) Specify the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.
conform - (Optional) Specify the action when a packet is mapped to the “green” color.
permit - Permits the packet.
replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
counter - (Optional) Specify the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specify that the ACL counter option will be enabled.
disable - Specify that the ACL counter option will be disabled.
exceed - Specify the action when a packet is mapped to the “yellow” color.
permit - Permits the packet.
replace_dscp - (Optional) Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
drop - Drops the packet.
counter - (Optional) Specify the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specify that the ACL counter option will be enabled.
disable - Specify that the ACL counter option will be disabled.
violate - Specify the action when a packet is mapped to the “red” color.
permit - Permits the packet.
replace_dscp - (Optional) Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
drop - Drops the packet.
counter - (Optional) Specify the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specify that the ACL counter option will be enabled.
disable - Specify that the ACL counter option will be disabled.

delete - Deletes the specified flow_meter.

Restrictions

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

Example

To configure a “two rate, three color” flow meter:

```
DES-3200-28P:admin#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000
cbs 2000 pir 2000 pbs 2000 color_blind conform permit counter enable exceed
permit replace_dscp 60 counter enable violate drop
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 2000
pir 2000 pbs 2000 color_blind conform permit counter enable exceed permit
replace_dscp 60 counter enable violate drop

Success.
DES-3200-28P:admin#
```

6-6 show flow_meter

Description

This command is used to display the flow-based metering (ACL Flow Metering) configuration.

Format

show flow_meter {[profile_id <value 1-4> | profile_name <name 32>] {access_id <value 1-256>}}

Parameters

profile_id - (Optional) Specify the profile ID. **<value 1-4>** - Enter the profile ID used here. This value must be between 1 and 4.
profile_name - (Optional) Specify the name of the profile. **<name 32>** - Enter the profile name used here. The maximum length is 32 characters.
access_id - (Optional) Specify the access ID. **<value 1-256>** - Enter the access ID used here. This value must be between 1 and 256.

Restrictions

None.

Example

To display the flow metering configuration:

```
DES-3200-28P:admin#show flow_meter
Command: show flow_meter

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

DES-3200-28P:admin#
```

6-7 config time_range

Description

This command is used to define a specific range of time to activate a function on the Switch by specifying which time range in a day and which days in a week are covered in the time range. Note that the specified time range is based on the SNTP time or the configured time. If this time is not available, the time range will not be met.

Format

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

Parameters

time_range - Specify the name of the time range settings. **<range_name 32>** - Enter the time range name used here. This name can be up to 32 characters long.
hours - Specify the time of a day. **start_time** - Specify the starting time of a day. **<time hh:mm:ss>** - Enter the starting time here. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter. **end_time** - Specify the ending time of a day. (24-hr time) **<time hh:mm:ss>** - Enter the ending time here. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter.
weekdays - Specify the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days. **<daylist>** - Enter the weekdays that will be included in this configuration here. For example, mon-fri (Monday to Friday). sun, mon, fri (Sunday, Monday and Friday)
delete - Deletes a time range profile. When a time_range profile has been associated with ACL entries, deleting the time_range profile will fail.

Restrictions

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

Example

To configure a time range named “1” that starts every Monday at 01:01:01am and ends at 02:02:02am:

```
DES-3200-28P:admin#config time_range 1 hours start_time 1:1:1 end_time 2:2:2
weekdays mon
Command: config time_range 1 hours start_time 1:1:1 end_time 2:2:2 weekdays mon

Success.

DES-3200-28P:admin#config time_range 1 delete
Command: config time_range 1 delete

Success.

DES-3200-28P:admin#
```

6-8 show time_range

Description

This command is used to display the current time range settings.

Format

show time_range

Parameters

None.

Restrictions

None.

Example

To display the current time range settings:

```
DES-3200-28P:admin#show time_range
Command: show time_range

Time Range Information
------------------------------
Range Name                : 1
Weekdays                  : Mon
Start Time                : 01:01:01
End Time                  : 02:01:01

Total Entries :1

DES-3200-28P:admin#
```

6-9 show current_config access_profile

Description

This command is used to display the ACL part of the current configuration, when logged in with user level privileges.

The overall current configuration can be displayed by using the show config command, which is accessible with administrator level privileges.

Format

show current_config access_profile

Parameters

None.

Restrictions

None.

Example

To display the ACL part of the current configuration:

```
DES-3200-28P:admin#show current_config access_profile
Command: show current_config access_profile

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

# ACL

create access_profile ethernet vlan profile_id 1
config access_profile profile_id 1 add access_id 1 ethernet vlan default port 1
permit

create access_profile ip source_ip_mask 255.255.255.255 profile_id 2
config access_profile profile_id 2 add access_id 1 ip source_ip 10.10.10.10
port 2 deny



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

DES-3200-28P:admin#
```

Chapter 7 Address Resolution Protocol (ARP) Command List

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

7-1 create arpentry

Description

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

Format

create arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - The IP address of the end node or station.
<macaddr> - The MAC address corresponding to the IP address above.

Restrictions

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

Example

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00-50-BA-00-07-36:

```
DES-3200-28P:admin#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DES-3200-28P:admin#
```

7-2 delete arpentry

Description

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

Format

delete arpentry [<ipaddr> | all]

Parameters

<ipaddr> - The IP address of the end node or station.
all - Delete all ARP entries.

Restrictions

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

Example

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DES-3200-28P:admin#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-3200-28P:admin#
```

7-3 config arpentry

Description

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

Format

config arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - The IP address of the end node or station.
<macaddr> - The MAC address corresponding to the IP address above.

Restrictions

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

Example

To configure a static ARP entry, whose IP address is 10.48.74.121, set its MAC address to 00-50-BA-00-07-37:

```
DES-3200-28P:admin#config arpentry 10.48.74.121 00-50-BA-00-07-37
Command: config arpentry 10.48.74.121 00-50-BA-00-07-37

Success.

DES-3200-28P:admin#
```

7-4 config arp_aging time

Description

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

Format

config arp_aging time <value 0-65535>

Parameters

<value 0-65535>- Enter the ARP age-out time, in minutes. This value must be between 0 and 65535 minutes.The default value is 20.

Restrictions

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

Example

To configure ARP aging time to 30 minutes:

```
DES-3200-28P:admin#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3200-28P:admin#
```

7-5 clear arptable

Description

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

Format

clear arptable

Parameters

None.

Restrictions

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

Example

To clear the ARP table:

```
DES-3200-28P:admin#clear arptable
Command: clear arptable

Success.

DES-3200-28P:admin#
```

7-6 show arpentry

Description

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

Format

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

Parameters

ipif - (Optional) The name of the IP interface the end node or station for which the ARP table entry was made, resides on. **<ipif_name 12>** - Enter the IP interface name here. This value can be up to 12 characters long.
ipaddress - (Optional) The IP address of the end node or station. **<ipaddr>** - Enter the IP address here.
static - (Optional) Display the static entries in the ARP table.
mac_address - (Optional) Displays the ARP entry by MAC address. **<macaddr>** - Enter the MAC address here.

Restrictions

None.

Example

To display the ARP table:

```
DES-3200-28P:admin#show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface       IP Address        MAC Address         Type
-------------  ---------------  -----------------  ---------------
System          10.0.0.0           FF-FF-FF-FF-FF-FF  Local/Broadcast
System          10.1.1.1           00-02-03-04-05-06  Static
System          10.1.1.2           00-02-03-04-05-06  Dynamic
System          10.1.1.3           00-02-03-04-05-06  Static
System          10.90.90.90        00-01-02-03-04-00  Local
System          10.255.255.255    FF-FF-FF-FF-FF-FF  Local/Broadcast

Total Entries: 6

DES-3200-28P:admin#
```

Chapter 8 ARP Spoofing Prevention Command List

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

8-1 config arp_spoofing_prevention

Description

This command is used to configure the spoofing prevention entry to prevent spoofing of MAC for the protected gateway. When an entry is created, those ARP packets whose sender IP matches the gateway IP of an entry, but source MAC field does not match the gateway MAC of the entry will be dropped by the system.

Format

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

Parameters

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

Restrictions

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

Example

To configure the ARP spoofing prevention entry:

```
DES-3200-28P:admin#config arp_spoofing_prevention add gateway_ip 10.254.254.251
gateway_mac 00-00-00-11-11-11 ports 1-2
Command: config arp_spoofing_prevention add gateway_ip 10.254.254.251 gateway_ma
c 00-00-00-11-11-11 ports 1-2

Success.

DES-3200-28P:admin#
```

8-2 show arp_spoofing_prevention

Description

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

Format

show arp_spoofing_prevention

Parameters

None.

Restrictions

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

Example

To display the ARP spoofing prevention entries:

```
DES-3200-28P:admin#show arp_spoofing_prevention
Command: show arp_spoofing_prevention

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

 Total Entries: 1


DES-3200-28P:admin#
```

Chapter 9 Auto-Configuration Command List

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

9-1 enable autoconfig

Description

This command is used to enable auto configuration. When enabled, during power on initialization, the Switch will get configure file path name and TFTP server IP address from the DHCP server. Then, the Switch will download the configuration file from the TFTP server for configuration of the system.

Format

enable autoconfig

Parameters

None.

Restrictions

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

Example

To enable autoconfig:

```
DES-3200-28P:admin#enable autoconfig
Command: enable autoconfig

Success.

DES-3200-28P:admin#
```

9-2 disable autoconfig

Description

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

Format

disable autoconfig

Parameters

None.

Restrictions

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

Example

To disable autoconfig:

```
DES-3200-28P:admin#disable autoconfig
Command: disable autoconfig

Success.

DES-3200-28P:admin#
```

9-3 show autoconfig

Description

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

Format

show autoconfig

Parameters

None.

Restrictions

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

Example

To show autoconfig status:

```
DES-3200-28P:admin#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled
Timeout         : 50 sec

DES-3200-28P:admin#
```

9-4 config autoconfig timeout

Description

This command is used to configure the timeout value. This timer is used to limit the length of time in getting configuration settings from the network. When timeout occurs, the auto configuration operation will be stopped and the local configuration file will be used to configure the system.

Format

config autoconfig timeout <value 1-65535>

Parameters

<value 1-65535> - Specify the timeout length in seconds. The default setting is 50 seconds.

Restrictions

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

Example

To configure auto configuration timeout:

```
DES-3200-28P:admin#config autoconfig timeout 60
Command: config autoconfig timeout 60

Success.

DES-3200-28P:admin#
```

Chapter 10 Basic Commands Command List

create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}
config account <username> {encrypt [plain_text | sha_1] <password>}
show account
delete account <username>
show switch
enable telnet {<tcp_port_number 1-65535>}
disable telnet
enable web {<tcp_port_number 1-65535>}
disable web
reboot {force_agree}
reset {[config | system]} {force_agree}
config firmware image <path_filename64>boot_up
create ipif <ipif_name 12> <network_address> <vlan_name 32> {state [enable|disable]}
config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable| disable]] |ipv4 state [enable | disable] | dhcp_option12 [hostname <hostname63> | clear_hostname | state [enable | disable]]]
delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]
enable ipif [<ipif_name 12> | all]
disable ipif [<ipif_name 12> | all]
show ipif {<ipif_name 12>}
enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
show ipif_ipv6_link_local_auto {<ipif_name 12>}

10-1 create account

Description

This command is used to create user accounts. The username is between 1 and 15 characters, the password is between 0 and 15 characters. It is case sensitive. The number of account (include admin and user) is up to 8.

Format

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

Parameters

admin - Specify the name of the admin account.
operator - Specify the name for a operator user account.
power_user – Specify the name for a Power-user account.
user - Specify the name of the user account.
<username 15> - Enter the username used here. This name can be up to 15 characters long.
encrypt - (Optional) Specify the encryption applied to the account. **plain_text** - 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.

Example

To create the admin-level user “dlink”:

```
DES-3200-28P:admin#create account admin dlink
Command: create account admin dlink

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

Success.

DES-3200-28P:admin#
```

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

```
DES-3200-28P:admin#create account user Remote-Manager
Command: create account user Remote-Manager

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

Success.

DES-3200-28P:admin#
```

10-2 config account

Description

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

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

Format

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

Parameters

<username> - Enter the user name of the account that has been defined.
encrypt - (Optional) Specify that the password will be encrypted. **plain_text** - Select to specify the password in plain text form. **sha_1** - Select to specify the password in the SHA-I enacrpted form. **<password>** - The password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The assword is case-sensitive.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the user password of “dlink” account:

```
DES-3200-28P:admin#config account dlink
Command: config account dlink

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

Success.

DES-3200-28P:admin#
```

To configure the user password of “administrator” account:

```
DES-3200-28P:admin#config account administrator encrypt sha_1
*@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq
Command: config account administrator encrypt sha_1
*@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq

Success.

DES-3200-28P:admin#
```

10-3 show account

Description

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

Format

show account

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the accounts that have been created:

```
DES-3200-28P:admin#show account
Command: show account

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

 Total Entries : 4

DES-3200-28P:admin#
```

10-4 delete account

Description

This command is used to delete an existing account.

Format

delete account <username>

Parameters

<username> - Name of the user who will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete the user account “System”:

```
DES-3200-28P:admin#delete account System
Command: delete account System

Success.

DES-3200-28P:admin#
```

10-5 show switch

Description

This command is used to display the Switch information.

Format

show switch

Parameters

None.

Restrictions

None.

Example

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

```
DES-3200-28P:admin#show switch
Command: show switch

Device Type                : DES-3200-28P Fast Ethernet Switch
MAC Address                : B8-A3-86-CF-1F-20
IP Address                 : 10.90.90.90 (Manual)
VLAN Name                  : default
Subnet Mask                : 255.0.0.0
Default Gateway            : 0.0.0.0
Boot PROM Version          : Build 4.00.001
Firmware Version           : Build 4.03.004
Hardware Version           : C1
Serial Number              : R3921BC000005
System Name                :
System Location            :
System Uptime              : 0 days, 0 hours, 2 minutes, 51 seconds
System Contact             :
Spanning Tree              : Disabled
GVRP                       : Disabled
IGMP Snooping              : Disabled
MLD Snooping               : Disabled
VLAN Trunk                 : Disabled
Telnet                     : Enabled (TCP 23)
Web                        : Enabled (TCP 80)
SNMP                       : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

10-6 enable telnet

Description

This command is used to enable TELNET and configure port number.

Format

enable telnet {<tcp_port_number 1-65535>}

Parameters

<tcp_port_number 1-65535> - (Optional) The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the TELNET protocol is 23.

Restrictions

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

Example

To enable TELNET and configure port number:

```
DES-3200-28P:admin#enable telnet 23
Command: enable telnet 23

Success.

DES-3200-28P:admin#
```

10-7 disable telnet

Description

This command is used to disable TELNET.

Format

disable telnet

Parameters

None.

Restrictions

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

Example

To disable TELNET:

```
DES-3200-28P:admin#disable telnet
Command: disable telnet

Success.

DES-3200-28P:admin#
```

10-8 enable web

Description

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

Format

enable web {<tcp_port_number 1-65535>}

Parameters

<tcp_port_number 1-65535> - (Optional) The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the WEB protocol is 80.

Restrictions

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

Example

To enable HTTP and configure port number:

```
DES-3200-28P:admin#enable web 80
Command: enable web 80

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

DES-3200-28P:admin#
```

10-9 disable web

Description

This command is used to disable HTTP.

Format

disable web

Parameters

None.

Restrictions

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

Example

To disable HTTP:

```
DES-3200-28P:admin#disable web
Command: disable web

Success.

DES-3200-28P:admin#
```

10-10 reboot

Description

This command is used to restart the Switch.

Format

reboot {force_agree}

Parameters

force_agree - (Optional) When force_agree is specified, the reboot command will be executed immediatedly without further confirmation.

Restrictions

Only Administrator-level users can issue this command.

Example

To reboot the Switch:

```
DES-3200-28P:admin#reboot
Command: reboot

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

10-11 reset

Description

This command is used to provide reset functions. The configuration setting will be reset to the default setting by the “reset config” command. For the “reset system” command, the device will store the reset setting in the NVRAM and then reboot the system. The “reset” command will not reset IP address, log, user accounts and banner configured on the system.

Format

reset {[config | system]} {force_agree}

Parameters

config - (Optional) If you specify the 'config' keyword , all parameters are reset to default settings. But device will not do save neither reboot.
system - (Optional) If you specify the 'system' keyword, all parameters are reset to default settings. Then the Switch will do factory reset, save and reboot.
force_agree - (Optional) When force_agree is specified, the reset command will be executed immediatedly without further confirmation.

Restrictions

Only Administrator-level users can issue this command.

Example

To reset the Switch:

```
DES-3200-28P:admin#reset system
Command: reset system

Are you sure you want to proceed with system reset?(y/n)
 y-(reset all include configuration, save, reboot )
 n-(cancel command) y
Reboot & Load Factory Default Configuration...

Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

10-12 config firmware image

Description

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

Note: DES-3200 Series with C1 hardware version support file system.

Format

config firmware image <path_filename64>boot_up

Parameters

<path_filename64> - Specify a firmware file on the device file system.
boot_up - Specify the firmware as the boot up firmware.

Restrictions

Only Administrator level can issue this command.

Example

To configure c:/DES3200_Run_4_00_014.had as the boot up image:

```
DES-3200-28P:admin#config firmware image c:/DES3200_Run_4_02_004.had boot_up
Command: config firmware image c:/DES3200_Run_4_02_004.had boot_up

Success.

DES-3200-28P:admin#
```

10-13 create ipif

Description

This command is used to create an IP interface.

Format

create ipif <ipif_name 12> <network_address> <vlan_name 32> {state [enable|disable]}

Parameters

ipif - Specify the name of the IP interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
<network_address> - Specify the IPv4 network address (xx.xx.xx.xx/xx). It specifies a host address and length of network mask.
<vlan_name 32> - Enter the VLAN name used here. This name can be up to 32 characters long.
state - (Optional) Specify the state of the IP interface. **enable** - Specify that the IP interface state will be enabled. **disable** - Specify that the IP interface state will be disabled.

Restrictions

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

Example

To create an IP interface:

```
DES-3200-28P:admin#create ipif Inter2 192.168.16.1/24 default state enable
Command: create ipif Inter2 192.168.16.1/24 default state enable

Success.

DES-3200-28P:admin#
```

10-14 config ipif

Description

This command is used to configure the IP interface.

Format

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable| disable]] |ipv4 state [enable | disable] | dhcp_option12 [hostname <hostname63> | clear_hostname | state [enable | disable]]]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
ipaddress - (Optional) Configures a network on an ipif. The address should specify a host address and length of network mask. Since an ipif can have only one IPv4 address, the new configured address will overwrite the original one. **<network_address>** - Enter the network address used here.
vlan - (Optional) Specify the name of the VLAN here. **<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long.
state - (Optional) Enable or disable the state of the interface. **enable** - Enable the state of the interface. **disable** - Disable the state of the interface.
bootp - Use BOOTP to obtain the IPv4 address.
dhcp - Use DHCP to obtain the IPv4 address.
ipv6 - Specify that the IPv6 configuration will be done. **ipv6address** - Specify the IPv6 network address. The address should specify a host address and length of network prefix. There can be multiple IPv6 addresses defined on an interface. Thus, as a new address is defined, it is added on this ipif. **<ipv6networkaddr>** - Enter the IPv6 address used here.
state - Specify that the IPv6 interface state will be set to enabled or disabled. **enable** - Specify that the IPv6 interface sate will be enabled. **disable** - Specify that the IPv6 interface sate will be disabled.
ipv4 - Specify that the IPv4 configuration will be done. **state** - Specify that the IPv4 interface state will be set to enabled or disabled. **enable** - Specify that the IPv4 interface sate will be enabled. **disable** - Specify that the IPv4 interface sate will be disabled.
dhcp_option12 - Specify the DHCP option 12. **hostname** - Specify the host name to be inserted in the DHCPDISCOVER and DHCPREQUEST message. **<hostname 63>** - Enter a name starting with a letter, end with a letter or digit, and have only letters, digits, and hyphen as interior characters; the maximal length is 63. **clear_hostname** - To clear the hostname setting. If host name is empty, system name will be used to encode option 12. The length of system is more than 63, the superfluous chars will be truncated. If system name is also empty, then product model name will be used to encode option 12. **state** - Enable or disable insertion of option 12 in the DHCPDISCOVER and DHCPREQUEST message. The state is disable by default. **enable** - Enable insertion of option 12 in the DHCPDISCOVER and DHCPREQUEST message. **disable** - Disable insertion of option 12 in the DHCPDISCOVER and DHCPREQUEST message.

Restrictions

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

Example

To configure an interface's IPv4 network address:

```
DES-3200-28P:admin#config ipif System ipaddress 192.168.69.123/24 vlan default
Command: config ipif System ipaddress 192.168.69.123/24 vlan default

Success.

DES-3200-28P:admin#
```

10-15 delete ipif

Description

This command is used to delete an IP interface.

Format

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

Parameters

ipif - Specify the name of the IP interface. **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
ipv6address – (Optional) Specify the IPv6 network address. The address should specify a host address and length of network prefix. There can be multiple IPv6 addresses defined on an interface. **<ipv6networkaddr>** - Enter the IPv6 address used here.
all – Specify that all the IP interfaces will be used.

Restrictions

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

Example

To delete an IP interface:

```
DES-3200-28P:admin#delete ipif newone
Command: delete ipif newone

Success.

DES-3200-28P:admin#
```

10-16 enable ipif

Description

This commands is used to enable the IP interface.

Format

enable ipif [<ipif_name 12> | all]

Parameters

ipif_name - Specify the name of the IP interface.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all – Specify that all the IP interfaces will be enabled.

Restrictions

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

Example

To enable an IP interface:

```
DES-3200-28P:admin#enable ipif newone
Command: enable ipif newone

Success.

DES-3200-28P:admin#
```

10-17 disable ipif

Description

This command is used to disable an IP interface.

Format

disable ipif [<ipif_name 12> | all]

Parameters

ipif_name - Specify the name of the IP interface.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all – Specify that all the IP interfaces will be disabled.

Restrictions

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

Example

To disable an IP interface:

```
DES-3200-28P:admin#disable ipif newone
Command: disable ipif newone

Success.

DES-3200-28P:admin#
```

10-18 show ipif

Description

This command is used to display an IP interface.

Format

show ipif {<ipif_name 12>}

Parameters

ipif_name - Specify the name of the IP interface.
<ipif_name 12> - (Optional) Enter the IP interface name used here. This name can be up to 12 characters long.

Restrictions

None.

Example

To display an IP interface:

```
DES-3200-28P:admin#show ipif
Command: show ipif

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


Total Entries: 1

DES-3200-28P:admin#
```

10-19 enable ipif_ipv6_link_local_auto

Description

This command is used to enable the auto configuration of link local address when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enable this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.

Format

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specify that all the IP interfaces will be used.

Restrictions

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

Example

To enable the IP interface for IPv6 link local automatic:

```
DES-3200-28P:admin#enable ipif_ipv6_link_local_auto newone
Command: enable ipif_ipv6_link_local_auto newone

Success.

DES-3200-28P:admin#
```

10-20 disable ipif_ipv6_link_local_auto

Description

This command is used to disable the auto configuration of link local address when no IPv6 address are configured.

Format

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specify that all the IP interfaces will be used.

Restrictions

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

Example

To disable the IP interface for IPv6 link local automatic:

```
DES-3200-28P:admin#disable ipif_ipv6_link_local_auto newone
Command: disable ipif_ipv6_link_local_auto newone

Success.

DES-3200-28P:admin#
```

10-21 show ipif_ipv6_link_local_auto

Description

This commands is used to display the link local address automatic configuration state.

Format

show ipif_ipv6_link_local_auto {<ipif_name 12>}

Parameters

<ipif_name 12> - (Optional) Enter the Ip interface name used here. This name can be up to 12 characters long.

Restrictions

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

Example

T o display the link local address automatic configuration state.

```
DES-3200-28P:admin#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System          Automatic Link Local Address: Disabled

DES-3200-28P:admin#
```

Chapter 11 BPDU Attack Protection Command List

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown} (1)
config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]
config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]
enable bpdu_protection
disable bpdu_protection
show bpdu_protection {ports {<portlist>}}

11-1 config bpdu_protection ports

Description

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

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

Format

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

Parameters

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

Restrictions

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

Example

To set the port state enable and drop mode:

```
DES-3200-28P:admin#config bpdu_protection ports 1 state enable mode drop
Commands: config bpdu_protection ports 1 state enable mode drop

Success.

DES-3200-28P:admin#
```

11-2 config bpdu_protection recovery_interval

Description

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

Format

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

Parameters

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

Restrictions

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

Example

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

```
DES-3200-28P:admin#config bpdu_protection recovery_timer 120
Commands: config bpdu_protection recovery_timer 120

Success.

DES-3200-28P:admin#
```

11-3 config bpdu_protection

Description

This command is used to configure the BPDU protection trap state or state for the Switch.

Format

config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]

Parameters

trap - To specify the trap state. **log** - To specify the log state.
none - Neither attack_detected nor attack_cleared is trapped or logged. **attack**_detected - Events will be logged or trapped when the BPDU attacks is detected. **attack**_cleared - Events will be logged or trapped when the BPDU attacks is cleared. **both** - The events of attack_detected and attack_cleared shall be trapped or logged.

Restrictions

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

Example

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

```
DES-3200-28P:admin#config bpdu_protection trap both
Commands: config bpdu_protection trap both

Success.

DES-3200-28P:admin#
```

11-4 enable bpdu_protection

Description

This command is used to enable BPDU protection function globally for the Switch.

Format

enable bpdu_protection

Parameters

None.

Restrictions

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

Example

To enable bpdu_protection function globally for the entire switch:

```
DES-3200-28P:admin#enable bpdu_protection
Commands: enable bpdu_protection

Success.

DES-3200-28P:admin#
```

11-5 disable bpdu_protection

Description

This command is used to disable BPDU protection function globally for the Switch.

Format

disable bpdu_protection

Parameters

None.

Restrictions

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

Example

To disable bpdu_protection function globally for the entire switch:

```
DES-3200-28P:admin#disable bpdu_protection
Commands: disable bpdu_protection

Success.

DES-3200-28P:admin#
```

11-6 show bpdu_protection

Description

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

Format

show bpdu_protection {ports {<portlist>}}

Parameters

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

Restrictions

None.

Example

To show the bpdu_protection for the entire switch:

```
DES-3200-28P:admin#show bpdu_protection
Commands: show bpdu_protection

BPDU Protection Global Settings
---------------------------------------
BPDU Protection status         : Enabled
BPDU Protection Recovery Time  : 60 seconds
BPDU Protection Trap State     : None
BPDU Protection Log State      : None


DES-3200-28P:admin#
```

To show the bpdu_protection status ports 1-12:

```
DES-3200-28P:admin#show bpdu_protection ports 1-12
Commands: show bpdu_protection ports 1-12

Port     State          Mode          Status
------ ------------ ----------- ----------
1        Enabled        shutdown     Normal
2        Enabled        shutdown     Normal
3        Enabled        shutdown     Normal
4        Enabled        shutdown     Normal
5        Enabled        shutdown     Under Attack
6        Enabled        shutdown     Normal
7        Enabled        shutdown     Normal
8        Enabled        shutdown     Normal
9        Enabled        shutdown     Normal
10       Enabled        Block        Normal
11       Disabled       shutdown     Normal
12       Disabled       shutdown     Normal

DES-3200-28P:admin#
```

Chapter 12 Cable Diagnostics Command List

cable_diag ports [<portlist> | all]

12-1 cable_diag ports

Description

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

The following test result can be displayed.

- **Open** - The cable in the error pair does not have a connection at the specified position.
- **Short** - The cable in the error pair has a short problem at the specified position.
- **Crosstalk** - The cable in the error pair has a crosstalk problem at the specified position.
- **Shutdown** - The remote partner is powered off.
- **Unknown** - The diagnosis does not obtain the cable status. Please try again.
- **OK** - The pair or cable has no error.
- **No cable** - The port does not have any cable connected to the remote partner.

When a port is in link-up status, the test will obtain the distance of the cable. Since the status is link-up, the cable will not have the short or open problem. But the test may still detect the crosstalk problem.

When a port is in link-down status, the link-down may be caused by many factors.

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

When the link partner is Fast Ethernet ports:

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

- When the **link partner is powered down with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error
- When there is **no link partner** with **no errors** and the **link is up**, this command can detect the cable length
- When there is **no link partner with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error

When the link partner is Gigabit Ethernet ports:

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

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

Format

cable_diag ports [<portlist> | all]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all – Specify that all the ports will be used for this configuration.

Restrictions

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

Example

Test the cable on port 1, 11, and 12:

```
DES-3200-28P:admin#cable_diag ports 1,11-12
Command: cable_diag ports 1,11-12

Perform Cable Diagnostics ...

Port      Type      Link Status    Test Result                Cable Length (M)
------  ----------  -------------  -------------------------  -----------------
1       100BASE-T   Link Up        OK                               4
11      100BASE-T   Link Down      No Cable                         -
12      100BASE-T   Link Down      No Cable                         -


DES-3200-28P:admin#
```

Chapter 13 Command Logging Command List

13-1 enable command logging

Description

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

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

Format

enable command logging

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the command logging function:

```
DES-3200-28P:admin#enable command logging
Command: enable command logging

Success.

DES-3200-28P:admin#
```

13-2 disable command logging

Description

This command is used to disable the command logging function.

Format

disable command logging

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the command logging:

```
DES-3200-28P:admin#disable command logging
Command: disable command logging

Success.

DES-3200-28P:admin#
```

13-3 show command logging

Description

This command is used to display the Switch's general command logging configuration status.

Format

show command logging

Parameters

None.

Restrictions

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

Example

To show the command logging configuration status:

```
DES-3200-28P:admin#show command logging
Command: show command logging

Command Logging State : Disabled

DES-3200-28P:admin#
```

Chapter 14 Compound Authentication Command List

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

14-1 enable authorization

Description

This command is used to enable authorization.

Format

enable authorization attributes

Parameters

None.

Restrictions

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

Example

This example sets authorization global state enabled:

```
DES-3200-28P:admin#enable authorization attributes
Command: enable authorization attributes

Success.

DES-3200-28P:admin#
```

14-2 disable authorization

Description

This command is used to disable authorization.

Format

disable authorization attributes

Parameters

None.

Restrictions

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

Example

This example sets authorization global state disabled:

```
DES-3200-28P:admin#disable authorization attributes
Command: disable authorization attributes

Success.

DES-3200-28P:admin#
```

14-3 show authorization

Description

This command is used to display authorization status.

Format

show authorization

Parameters

None.

Restrictions

None.

Example

This example displays authorization status:

```
DES-3200-28P:admin#show authorization
Command: show authorization

Authorization for Attributes: Enabled.

DES-3200-28P:admin#
```

14-4 config authentication server failover

Description

This command is used to configure authentication server failover function.

Format

config authentication server failover [local | permit | block]

Parameters

local - Use local DB to authenticate the client.
permit - The client is always regarded as authenticated.
block - Block the client (Default setting).

Restrictions

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

Example

Set authentication server auth fail over state:

```
DES-3200-28P:admin#config authentication server failover local
Command: config authentication server failover local

Success.

DES-3200-28P:admin#
```

14-5 show authentication

Description

This command is used to display authentication global configuration.

Format

show authentication

Parameters

None.

Restrictions

None.

Example

To show authentication global configuration:

```
DES-3200-28P:admin#show authentication
Command: show authentication

Authentication Server Failover: Local.

DES-3200-28P:admin#
```

Chapter 15 Configuration Command List

show config [effective | modified | current_config | boot_up | file <pathname 64>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}
config configuration <pathname 64> [boot_up | active]
save {[config <pathname 64> | log | all]}
show boot_file

15-1 show config

Description

This command is used to display the content of the current configuration, the configuration to be used in next boot, or the configuration file specified by the command.

The output stream of the configuration data can be filtered by the expression specified at the end of the command. The expression can contain up to three multiple filter evaluations. A filter evaluation begins with a filter type (include, exclude, and begin), followed by up to three filter strings (ex: “stp”). A filter string is enclosed by symbol ". The following describes the meaning of the each filter type.

include: includes lines that contain the specified filter string.

exclude: excludes lines that contain the specified filter string

begin: The first line that contains the specified filter string will be the first line of the output.

The relationship of multiple filter strings following the same filter type is OR. That is, one line is qualified if one of specified filter strings is matched.

If more than one filter evaluation is specified; the output of filtered by the former evaluation will be used as the input of the latter evaluation.

Format

show config [effective | modified | current_config | boot_up | file <pathname 64>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}

Parameters

effective - Show only commands which affects the behavior of the device. For example, if STP is disabled, then for STP configuration, only “STP is disabled” is displayed. All other lower level

setting regarding STP is not displayed. The lower level setting will only be displayed when the higher level setting is enabled. **Note:** This parameter is only for the current configuration.
modified - Show only the commands which are not default setting. **Note:**This parameter is only for the current configuration.
current_config - Specify the current configuration.
boot_up - Specify the list of the bootup configuration.
file - Specify to display the configuration file. **<pathname 64>** - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, the boot up configuration is implied. This name can be up to 64 characters long.
include - (Optional) Include lines that contain the specified filter string. **exclude** - (Optional) Exclude lines that contain the specified filter string. **begin** - (Optional) The first line that contains the specified filter string will be the first line of the output. **<filter_string 80>** - A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long. **<filter_string 80>** - (Optional) A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long. **<filter_string 80>** - (Optional) A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long.
include - (Optional) Include lines that contain the specified filter string. **exclude** - (Optional) Exclude lines that contain the specified filter string. **begin** - (Optional) The first line that contains the specified filter string will be the first line of the output. **<filter_string 80>** - A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long. **<filter_string 80>** - (Optional) A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long. **<filter_string 80>** - (Optional) A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long.
include - (Optional) Include lines that contain the specified filter string. **exclude** - (Optional) Exclude lines that contain the specified filter string. **begin** - (Optional) The first line that contains the specified filter string will be the first line of the output. **<filter_string 80>** - A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long. **<filter_string 80>** - (Optional) A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long. **<filter_string 80>** - (Optional) A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long.

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#show config modified
Command: show config modified

#------------------------------------------------------------------------
#                      DES-3200-28P Fast Ethernet Switch
#                                Configuration
#
#                            Firmware: Build 4.03.004
#           Copyright(C) 2012 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------


# DEVICE


# BASIC

# ACCOUNT LIST
create account admin admin
admin
admin


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

15-2 config configuration

Description

This command is used to select a configuration file as the next boot up configuration or to apply a specific configuration to the system. This command is required when multiple configuration files are supported.

Note: DES-3200 Series with C1 hardware version support file system.

Format

config configuration <pathname 64> [boot_up | active]

Parameters

<pathname 64> - Specify a configuration file on the device file system.
boot_up - Specify it as a boot up file.
active - Specify to apply the configuration.

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#config configuration config.cfg boot_up
Command: config configuration config.cfg boot_up

Success.
DES-3200-28P:admin#
```

15-3 save

Description

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

Format

save {[config <pathname 64> | log | all]}

Parameters

config - (Optional) Specify to save the configuration to a file. **<pathname64>** - The pathname specifies the absolute pathname on the device file system. If pathname is not specified, it refers to the boot up configuration file.
log - (Optional) Specify to save the log.
all - (Optional) Specify to save the configuration and the log.

Restrictions

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

Example

To save the configuration:

```
DES-3200-28P:admin#save config c:/3200.cfg
Command: save config c:/3200.cfg

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

DES-3200-28P:admin#
```

15-4 show boot file

Description

This command is used to display the configuration file and firmware image assigned as boot up files.

Format

show boot_file

Parameters

None.

Restrictions

None.

Example

To display the boot file:

```
DES-3200-28P:admin#show boot_file
Command: show boot_file

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

DES-3200-28P:admin#
```

Chapter 16 Connectivity Fault Management (CFM) Command List

create cfm md <string 22> {md_index <uint 1-4294967295>} level <int 0-7>
config cfm md [<string 22> | md_index <uint 1-4294967295>] {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}
create cfm ma <string 22> {ma_index <uint 1-4294967295>} md [<string 22> | md_index <uint 1-4294967295>]
config cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>] {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}
create cfm mep <string 32> mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] direction [inward | outward] port <port>
config cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centisecond 250 -1000> | alarm_reset_time <centisecond 250-1000>}
delete cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]]
delete cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>]
delete cfm md [<string 22> | md_index <uint 1-4294967295>]
enable cfm
disable cfm
config cfm ports <portlist> state [enable | disable]
show cfm ports <portlist>
show cfm {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>]}}
show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}
cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}
cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {ttl <int 2-255> | pdu_priority <int 0-7>}
show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {trans_id <uint>}
delete cfm linktrace {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm mipccm
config cfm mp_ltr_all [enable | disable]
show cfm mp_ltr_all
show cfm remote_mep [mepname <string 32> | md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191>] remote_mepid <int 1-8191>
show cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

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

16-1 create cfm md

Description

This command is used to create a maintenance domain.

Format

create cfm md <string 22> {md_index <uint 1-4294967295>} level <int 0-7>

Parameters

<string 22> - Enter the maintenance domain name. This name can be up to 22 characters long.
md_index - (Optional) Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
level - Specify the maintenance domain level. **<int 0-7>** - Enter the maintenance domain level here. This value must be between 0 and 7.

Restrictions

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

Example

To create a maintenance domain called “op_domain” and assign a maintenance domain level of “2”:

```
DES-3200-28P:admin#create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

DES-3200-28P:admin#
```

16-2 config cfm md

Description

This command is used to configure the parameters of a maintenance domain. The creation of MIPs on an MA is useful to trace the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP.

Format

config cfm md [<string 22> | md_index <uint 1-4294967295>] {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}

Parameters

<string 22> - Enter the maintenance domain name. This name can be up to 22 characters long.
md_index - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
mip - (Optional) This is the control creations of MIPs. **none** - Do not create MIPs. This is the default value. **auto** - MIPs can always be created on any ports in this MD, if that port is not configured with an MEP of this MD. For the intermediate switch in an MA, the setting must be automatic in order for the MIPs to be created on this device. **explicit** - MIPs can be created on any ports in this MD, only if the next existent lower level has an MEP configured on that port, and that port is not configured with an MEP of this MD.
sender_id - (Optional) This is the control transmission of the sender ID TLV. **none** - Do not transmit the sender ID TLV. This is the default value. **chassis** - Transmit the sender ID TLV with the chassis ID information. **manage** - Transmit the sender ID TLV with the managed address information. **chassis_manage** - Transmit sender ID TLV with chassis ID information and manage address information.

Restrictions

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

Example

To configure the maintenance domain called “op_domain” and specify the explicit option for creating MIPs:

```
DES-3200-28P:admin#config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DES-3200-28P:admin#
```

16-3 create cfm ma

Description

This command is used to create a maintenance association. Different MAs in an MD must have different MA Names. Different MAs in different MDs may have the same MA Name.

Format

create cfm ma <string 22> {ma_index <uint 1-4294967295>} md [<string 22> | md_index <uint 1-4294967295>]

Parameters

<string 22> - Enter the maintenance association name. This name can be up to 22 characters long.
ma_index - (Optional) Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

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

Restrictions

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

Example

To create a maintenance association called “op1” and assign it to the maintenance domain “op_domain”:

```
DES-3200-28P:admin#create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DES-3200-28P:admin#
```

16-4 config cfm ma

Description

This command is used to configure the parameters of a maintenance association. The MEP list specified for an MA can be located in different devices. MEPs must be created on the ports of these devices explicitly. An MEP will transmit a CCM packet periodically across the MA. The receiving MEP will verify these received CCM packets from the other MEPs against this MEP list for the configuration integrity check.

Format

config cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>] {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}

Parameters

<string 22> - Enter the maintenance association name. This name can be up to 22 characters long.
ma_index - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
md - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long. **md_index** - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
vlanid - (Optional) Specify the VLAN Identifier. Different MAs must be associated with different

VLANs. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
mip - (Optional) This is the control creation of MIPs. **none** - Specify not to create MIPs. **auto** - MIPs can always be created on any ports in this MA, if that port is not configured with an MEP of that MA. **explicit** - MIP can be created on any ports in this MA, only if the next existing lower level has an MEP configured on that port, and that port is not configured with an MEP of this MA. **defer** - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
sender_id - (Optional) This is the control transmission of the sender ID TLV. **none** - Do not transmit the sender ID TLV. This is the default value. **chassis** - Transmit the sender ID TLV with the chassis ID information. **manage** - Transmit the sender ID TLV with the manage address information. **chassis_manage** - Transmit the sender ID TLV with the chassis ID information and the manage address information. **defer** - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
ccm_interval - (Optional) This is the CCM interval. **10ms** - Specify that the CCM interval will be set to 10 milliseconds. Not recommended. **100ms** - Specify that the CCM interval will be set to 100 milliseconds. Not recommended. **1sec** - Specify that the CCM interval will be set to 1 second. **10sec** - Specify that the CCM interval will be set to 10 seconds. This is the default value. **1min** - Specify that the CCM interval will be set to 1 minute. **10min** - Specify that the CCM interval will be set to 10 minutes.
mepid_list - (Optional) This is to specify the MEPIDs contained in the maintenance association. The range of the MEPID is 1-8191. **add** - Specify to add MEPID(s). **delete** - Specify to delete MEPID(s). By default, there is no MEPID in a newly created maintenance association. **<mepid_list>** - Enter the MEP ID list here.

Restrictions

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

Example

To configure a CFM MA:

```
DES-3200-28P:admin#config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec
Command: config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec

Success.

DES-3200-28P:admin#
```

16-5 create cfm mep

Description

This command is used to create an MEP. Different MEPs in the same MA must have a different MEPID. MD name, MA name, and MEPID that together identify a MEP.

Different MEPs on the same device must have a different MEP name. Before creating an MEP, its MEPID should be configured in the MA's MEPID list.

Format

create cfm mep <string 32> mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] direction [inward | outward] port <port>

Parameters

<string 32> - Enter the MEP name used. It is unique among all MEPs configured on the device.This name can be up to 32 characters long.
mepid - Specify the MEP ID. It should be configured in the MA's MEPID list. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
md - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long. **md_index** - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
ma - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long. **ma_index** - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
direction - This is the MEP direction. **inward** - Specify the inward facing (up) MEP. **outward** - Specify the outward facing (down) MEP.
port - Specify the port number. This port should be a member of the MA's associated VLAN. **<port>** - Enter the port number used here.

Restrictions

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

Example

To create a CFM MEP:

```
DES-3200-28P:admin#create cfm mep mep1 mepid 1 md op_domain ma op1 direction
inward port 2
Command: create cfm mep mep1 mepid 1 md op_domain ma op1 direction inward port
2

Success.

DES-3200-28P:admin#
```

16-6 config cfm mep

Description

This command is used to configure the parameters of an MEP.

An MEP may generate 5 types of Fault Alarms, as shown below by their priorities from high to low:

- Cross-connect CCM Received: priority 5
- Error CCM Received: priority 4

- Some Remote MEPs Down: priority 3
- Some Remote MEP MAC Status Errors: priority 2
- Some Remote MEP Defect Indications: priority 1

If multiple types of the fault occur on an MEP, only the fault with the highest priority will be alarmed.

Format

config cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centisecond 250 -1000> | alarm_reset_time <centisecond 250-1000>}

Parameters

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

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

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

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

pdu_priority - (Optional) The 802.1p priority is set in the CCMs and the LTMs messages transmitted by the MEP. The default value is 7.
- **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.

fault_alarm - (Optional) This is the control types of the fault alarms sent by the MEP.
- **all** - All types of fault alarms will be sent.
- **mac_status** - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP MAC Status Errors” are sent.
- **remote_ccm** - Only the fault alarms whose priority is equal to or higher than “Some Remote MEPs Down” are sent.
- **error_ccm** - Only the fault alarms whose priority is equal to or higher than “Error CCM Received” are sent.
- **xcon_ccm** - Only the fault alarms whose priority is equal to or higher than “Cross-connect CCM Received” are sent.
- **none** - No fault alarm is sent. This is the default value.

alarm_time - (Optional) This is the time that a defect must exceed before the fault alarm can be sent. The unit is centisecond, the range is 250-1000. The default value is 250.
- **<centisecond 250-1000>** - Enter the alarm time value here. This value must be between 250 and 1000 centiseconds.

alarm_reset_time - (Optional) This is the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is centisecond, the range is 250-1000. The default value is 1000.
<centisecond 250-1000> - Enter the alarm reset time value here. This value must be between 250 and 1000 centiseconds.

Restrictions

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

Example

To configure a CFM MEP:

```
DES-3200-28P:admin#config cfm mep mepname mep1 state enable ccm enable
Command: config cfm mep mepname mep1 state enable ccm enable

Success.

DES-3200-28P:admin#
```

16-7 delete cfm mep

Description

This command is used to delete a previously created MEP.

Format

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

Parameters

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

Restrictions

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

Example

To delete a CFM MEP:

```
DES-3200-28P:admin#delete cfm mep mepname mep1
Command: delete cfm mep mepname mep1

Success.

DES-3200-28P:admin#
```

16-8 delete cfm ma

Description

This command is used to delete a created maintenance association. All MEPs created in the maintenance association will be deleted automatically.

Format

delete cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>]

Parameters

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

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

Restrictions

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

Example

To delete a CFM MA:

```
DES-3200-28P:admin#delete cfm ma op1 md op_domain
Command: delete cfm ma op1 md op_domain

Success.

DES-3200-28P:admin#
```

16-9 delete cfm md

Description

This command is used to delete a previously created maintenance domain. All the MEPs and maintenance associations created in the maintenance domain will be deleted automatically.

Format

delete cfm md [<string 22> | md_index <uint 1-4294967295>]

Parameters

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

Restrictions

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

Example

To delete a CFM MD:

```
DES-3200-28P:admin#delete cfm md op_domain
Command: delete cfm md op_domain

Success.

DES-3200-28P:admin#
```

16-10 enable cfm

Description

This command is used to enable the CFM globally.

Format

enable cfm

Parameters

None.

Restrictions

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

Example

To enable the CFM globally:

```
DES-3200-28P:admin#enable cfm
Command: enable cfm

Success.

DES-3200-28P:admin#
```

16-11 disable cfm

Description

This command is used to disable the CFM globally.

Format

disable cfm

Parameters

None.

Restrictions

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

Example

To disable the CFM globally:

```
DES-3200-28P:admin#disable cfm
Command: disable cfm

Success.

DES-3200-28P:admin#
```

16-12 config cfm ports

Description

This command is used to enable or disable the CFM function on a per-port basis. By default, the CFM function is disabled on all ports.

If the CFM is disabled on a port:

1. MIPs are never created on that port.
2. MEPs can still be created on that port, and the configuration can be saved.
3. MEPs created on that port can never generate or process CFM PDUs. If the user issues a Loopback or Link trace test on those MEPs, it will prompt the user to inform them that the CFM function is disabled on that port.

Format

config cfm ports <portlist> state [enable | disable]

Parameters

<portlist> - Enter the list of ports used for this configuration.
state - Specify that the the CFM function will be enabled or disabled. **enable** - Specify that the CFM function will be enabled. **disable** - Specify that the CFM function will be disabled.

Restrictions

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

Example

To configure the CFM ports:

```
DES-3200-28P:admin#config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

DES-3200-28P:admin#
```

16-13 show cfm ports

Description

This command is used to show the CFM state of specified ports.

Format

show cfm ports <portlist>

Parameters

<portlist> - Enter the list of logical ports.

Restrictions

None.

Example

To show the CFM ports:

```
DES-3200-28P:admin#show cfm ports 3-6
Command: show cfm ports 3-6

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

DES-3200-28P:admin#
```

16-14 show cfm

Description

This command is used to show the CFM configuration.

Format

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

Parameters

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

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

Restrictions

None.

Example

To show the CFM configuration:

```
DES-3200-28P:admin#show cfm
Command: show cfm
```

```
CFM State: Enabled

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

DES-3200-28P:admin#show cfm md op_domain
Command: show cfm md op_domain

MD Index    : 1
MD Name     : op_domain
MD Level    : 2
MIP Creation: Explicit
SenderID TLV: None

MA Index    MA Name                 VID
----------  ----------------------  ----
1           op1                     1

DES-3200-28P:admin#show cfm md op_domain ma op1
Command: show cfm md op_domain ma op1

MA Index    : 1
MA Name     : op1
MA VID      : 1
MIP Creation: Defer
CCM Interval: 1 second
SenderID TLV: Defer
MEPID List  : 1

MEPID  Direction  Port   Name         MAC Address
-----  ---------  -----  -----------  -----------------
1      Inward     2      mep1         00-01-02-03-04-02


DES-3200-28P:admin#show cfm mepname mep1
Command: show cfm mepname mep1

Name                : mep1
MEPID               : 1
Port                : 2
Direction           : Inward
CFM Port Status     : Disabled
MAC Address         : 00-01-02-03-04-02
MEP State           : Enabled
CCM State           : Enabled
PDU Priority        : 7
Fault Alarm         : Disabled
Alarm Time          : 250 centisecond((1/100)s)
Alarm Reset Time    : 1000 centisecond((1/100)s)
Highest Fault       : None
Out-of-Sequence CCMs: 0 received
```

```
Cross-connect CCMs  : 0 received
Error CCMs          : 0 received
Normal CCMs         : 0 received
Port Status CCMs    : 0 received
If Status CCMs      : 0 received
CCMs transmitted    : 0
In-order LBRs       : 0 received
Out-of-order LBRs   : 0 received
Next LTM Trans ID   : 0
Unexpected LTRs     : 0 received
LBMs Transmitted    : 0


Remote
MEPID  MAC Address       Status RDI PortSt  IfSt       Detect Time
------ ----------------- ------ --- ------- ---------- -------------------
2      FF-FF-FF-FF-FF-FF FAILED No  No      No         2011-07-13 12:00:00

DES-3200-28P:admin#
```

16-15 show cfm fault

Description

This command is used to display all the fault conditions detected by the MEPs contained in the specified MA or MD. This display provides the overview of the fault status by MEPs.

Format

show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>]}}

Parameters

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

Restrictions

None.

Example

To show the CFM faults:

```
DES-3200-28P:admin#show cfm fault
Command: show cfm fault

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

DES-3200-28P:admin#
```

16-16 show cfm port

Description

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

Format

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

Parameters

<port> - Enter the port number used here.
level - (Optional) Specify the MD Level. If not specified, all levels are shown. **<int 0-7>** - Enter the MD level value here. This value must be between 0 and 7.
direction - (Optional) Specify the MEP direction. **inward** - Specify that the MEP direction will be inward facing. **outward** - Specify that the MEP direction will be outward facing. If not specified, both directions and the MIP are shown.
vlanid - (Optional) Specify the VLAN identifier. If not specified, all VLANs are shown. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

Restrictions

None.

Example

To show the MEPs and MIPs created on a port:

```
DES-3200-28P:admin#show cfm port 2
Command: show cfm port 2

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

DES-3200-28P:admin#
```

16-17 cfm loopback

Description

This command is used to start a CFM loopback test. You can press Ctrl+C to exit the loopback test. The MAC address represents the destination MEP or MIP that can be reached by this MAC address. The MEP represents the source MEP to initiate the loopback message.

Format

cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}

Parameters

<macaddr> - Enter the destination MAC address here.
mepname - Specify the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
mepid - Specify the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191. **md** - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long. **md_index** - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295. **ma** - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long. **ma_index** - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
num - (Optional) Number of LBMs to be sent. The default value is 4. **<int 1-65535>** - Enter the number of LBMs to be sent here. This value must be between 1 and 65535.
length - (Optional) The payload length of the LBM to be sent. The default is 0. **<int 0-1500>** - Enter the payload length here. This value must be between 0 and 1500.
pattern - (Optional) An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included. **<string 1500>** - Enter the pattern used here. This value can be up to 1500 characters long.
pdu_priority - (Optional) The 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA. **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.

Restrictions

None.

Example

To transmit a LBM:

```
DES-3200-28P:admin#cfm loopback 32-00-70-89-31-06 mepname mep1
Command: cfm loopback 32-00-70-89-31-06 mepname mep1

Reply from 32-00-70-89-31-06: bytes=0 time=50ms
Reply from 32-00-70-89-31-06: bytes=0 time=50ms
Reply from 32-00-70-89-31-06: bytes=0 time=50ms
Reply from 32-00-70-89-31-06: bytes=0 time=50ms

CFM loopback statistics for 32-00-70-89-31-06:
        Packets: Sent=4, Received=4, Lost=0(0% loss).

DES-3200-28P:admin#"
```

16-18 cfm linktrace

Description

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

Format

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

Parameters

<macaddr> - Specify the destination MAC address.

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

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

ttl - (Optional) Specify the link trace message TTL value. The default value is 64.
- **<int 2-255>** - Enter the link trace message TTL value here. This value must be between 2 and 255.

pdu_priority - (Optional) The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA.
- **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.

Restrictions

None.

Example

To transmit an LTM:

```
DES-3200-28P:admin#cfm linktrace 00-01-02-03-04-05 mepname mep1
Command: cfm linktrace 00-01-02-03-04-05 mepname mep1

Transaction ID: 26
Success.

DES-3200-28P:admin#
```

16-19 show cfm linktrace

Description

This command is used to show the link trace responses. The maximum link trace responses a device can hold is 128.

Format

show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {trans_id <uint>}

Parameters

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

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

trans_id - (Optional) Specify the identifier of the transaction displayed.
- **<uint>** - Enter the transaction ID used here.

Restrictions

None.

Example

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

```
DES-3200-28P:admin#show cfm linktrace mepname mep1 trans_id 26
Command: show cfm linktrace mepname mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 32-00-70-89-31-06
Start Time    : 2011-11-22 16:05:08

Hop  MEPID  Ingress MAC Address  Egress MAC Address   Forwarded  Relay Action
---  -----  ------------------  ------------------  ---------  ------------
1    -      00-00-00-00-00-00    32-00-70-89-41-06    Yes        FDB
2    -      00-32-28-40-09-07    00-32-28-40-09-05    Yes        FDB
3    2      00-00-00-00-00-00    32-00-70-89-31-06    No         Hit

DES-3200-28P:admin#″
```

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

```
DES-3200-28P:admin#show cfm linktrace mepname mep1 trans_id 27
Command: show cfm linktrace mepname mep1 trans_id 27

Transaction ID: 27
From MEP mep1 to 32-00-70-89-31-06
Start Time    : 2011-11-22 16:28:56

Hop  MEPID  Ingress MAC Address  Egress MAC Address   Forwarded  Relay Action
---  -----  ------------------  ------------------  ---------  ------------
1    -      00-00-00-00-00-00    32-00-70-89-41-06    Yes        FDB
2    -      00-32-28-40-09-07    00-32-28-40-09-05    Yes        FDB
3    2      00-00-00-00-00-00    32-00-70-89-31-06    No         Hit

DES-3200-28P:admin#″
```

16-20 delete cfm linktrace

Description

This command is used to delete the stored link trace response data that have been initiated by the specified MEP.

Format

delete cfm linktrace {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}

Parameters

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

	be between 1 and 4294967295. **ma** - (Optional) Specify the maintenance association name. **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long. **ma_index** - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295. **mepid** - (Optional) Specify the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
mepname - (Optional) Specify the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.	

Restrictions

None.

Example

To delete the CFM link trace reply:

```
DES-3200-28P:admin#delete cfm linktrace mepname mep1
Command: delete cfm linktrace mepname mep1

Success.

DES-3200-28P:admin#
```

16-21 show cfm mipccm

Description

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

Format

show cfm mipccm

Parameters

None.

Restrictions

None.

Example

To show MIP CCM database entries:

```
DES-3200-28P:admin#show cfm mipccm
Command: show cfm mipccm

MA          VID   MAC Address        Port
----------  ----  -----------------  -----
opma        1     xx-xx-xx-xx-xx-xx  2
opma        1     xx-xx-xx-xx-xx-xx  3

Total: 2

DES-3200-28P:admin#
```

16-22 config cfm mp_ltr_all

Description

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

Format

config cfm mp_ltr_all [enable | disable]

Parameters

enable - Specify that the MP's reply to the LTR function will be set to all.
disable - Disable sending the all MPs replay LTRs function.

Restrictions

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

Example

To enable the "all MPs reply LTRs" function:

```
DES-3200-28P:admin#config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

DES-3200-28P:admin#
```

16-23 show cfm mp_ltr_all

Description

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

Format

show cfm mp_ltr_all

Parameters

None.

Restrictions

None.

Example

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

```
DES-3200-28P:admin#show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Disabled

DES-3200-28P:admin#
```

16-24 show cfm remote_mep

Description

This command is used to show remote MEPs.

Format

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

Parameters

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

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

remote_mepid - Specify the Remote MEP ID used.
- **<int 1-8191>** - Enter the remote MEP ID used here. This value must be between 1 and 8191.

Restrictions

None.

Example

To show the CFM Remote MEP information:

```
DES-3200-28P:admin#show cfm remote_mep mepname mep1 remote_mepid 2
Command: show cfm remote_mep mepname mep1 remote_mepid 2

Remote MEPID             : 2
MAC Address              : 00-11-22-33-44-02
Status                   : OK
RDI                      : Yes
Port State               : Blocked
Interface Status         : Down
Last CCM Serial Number   : 1000
Sender Chassis ID        : 00-11-22-33-44-00
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time              : 2008-01-01 12:00:00

DES-3200-28P:admin#
```

16-25 show cfm pkt_cnt

Description

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

Format

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

Parameters

ports - (Optional) Specify the port counters to show. If not specified, all ports will be shown. **<portlist>** - Enter the list of ports used for this configuration here. **rx** - (Optional) Specify to display the RX counter. **tx** - (Optional) Specify to display the TX counter. If not specified, both of them will be shown.
rx - (Optional) Specify to display the RX counter.
tx - (Optional) Specify to display the TX counter. If not specified, both of them will be shown.
ccm - (Optional) Specify the CCM RX counters.

Restrictions

None.

Example

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

```
DES-3200-28P:admin#show cfm pkt_cnt
Command: show cfm pkt_cnt

CFM RX Statistics
```

```
-------------------------------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM      LTR      LTM      VidDrop  OpcoDrop
----- -------- -------- -------- -------- -------- -------- -------- --------
all   2446     2434     0        9        0        3        0        0
1     2446     2434     0        9        0        3        0        0
2     0        0        0        0        0        0        0        0
3     0        0        0        0        0        0        0        0
4     0        0        0        0        0        0        0        0
5     0        0        0        0        0        0        0        0
6     0        0        0        0        0        0        0        0
7     0        0        0        0        0        0        0        0
8     0        0        0        0        0        0        0        0
9     0        0        0        0        0        0        0        0
10    0        0        0        0        0        0        0        0
11    0        0        0        0        0        0        0        0
12    0        0        0        0        0        0        0        0
13    0        0        0        0        0        0        0        0
14    0        0        0        0        0        0        0        0
15    0        0        0        0        0        0        0        0
16    0        0        0        0        0        0        0        0
17    0        0        0        0        0        0        0        0
18    0        0        0        0        0        0        0        0
19    0        0        0        0        0        0        0        0
20    0        0        0        0        0        0        0        0
21    0        0        0        0        0        0        0        0
22    0        0        0        0        0        0        0        0
23    0        0        0        0        0        0        0        0
24    0        0        0        0        0        0        0        0
25    0        0        0        0        0        0        0        0
26    0        0        0        0        0        0        0        0
27    0        0        0        0        0        0        0        0
28    0        0        0        0        0        0        0        0

CFM TX Statistics
-------------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM      LTR      LTM
----- -------- -------- -------- -------- -------- --------
all   1974     1974     0        0        0        0
1     1974     1974     0        0        0        0
2     0        0        0        0        0        0
3     0        0        0        0        0        0
4     0        0        0        0        0        0
5     0        0        0        0        0        0
6     0        0        0        0        0        0
7     0        0        0        0        0        0
8     0        0        0        0        0        0
9     0        0        0        0        0        0
10    0        0        0        0        0        0
11    0        0        0        0        0        0
12    0        0        0        0        0        0
13    0        0        0        0        0        0
14    0        0        0        0        0        0
```

```
15    0         0         0         0         0         0
16    0         0         0         0         0         0
17    0         0         0         0         0         0
18    0         0         0         0         0         0
19    0         0         0         0         0         0
20    0         0         0         0         0         0
21    0         0         0         0         0         0
22    0         0         0         0         0         0
23    0         0         0         0         0         0
24    0         0         0         0         0         0
25    0         0         0         0         0         0
26    0         0         0         0         0         0
27    0         0         0         0         0         0
28    0         0         0         0         0         0

DES-3200-28P:admin#show cfm pkt_cnt ccm
Command: show cfm pkt_cnt ccm

CCM RX counters:
XCON   = Cross-connect CCMs
Error  = Error CCMs
Normal = Normal CCMs

MEP Name    VID  Port  Level  Direction  XCON       Error      Normal
----------- ---- ----- ------ ---------- ---------- ---------- ----------
1           1    1     1      Inward     0          0          0
28mep       45   3     7      Inward     0          0          2438
                               ------------------------------------------
                               Total:     0          0          2438

DES-3200-28P:admin#
```

16-26 clear cfm pkt_cnt

Description

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

Format

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

Parameters

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

Restrictions

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

Example

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

```
DES-3200-28P:admin#clear cfm pkt_cnt
Command: clear cfm pkt_cnt

Success.

DES-3200-28P:admin#clear cfm pkt_cnt ccm
Command: clear cfm pkt_cnt ccm

Success.

DES-3200-28P:admin#
```

Chapter 17 CPU Interface Filtering Command List

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

17-1 create cpu access_profile

Description

This command is used to create CPU access list profiles.

Format

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

<hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]

Parameters

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

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

ip - Specify that the profile type will be IP.
- **vlan** - (Optional) Specify a VLAN mask.
- **source_ip_mask** - (Optional) Specify an IP source submask.
  - **<netmask>** - Enter the IP source submask here.
- **destination_ip_mask** - (Optional) Specify an IP destination submask.
  - **<netmask>** - Enter the IP destination submask here.
- **dscp** - (Optional) Specify the DSCP mask.
- **icmp** - (Optional) Specify that the rule applies to ICMP traffic.
  - **type** - (Optional) Specify that the rule applies to ICMP type traffic.
  - **code** - (Optional) Specify that the rule applies to ICMP code traffic.
- **igmp** - (Optional) Specify that the rule applies to IGMP traffic.
  - **type** - (Optional) Specify that the rule applies to IGMP type traffic.
- **tcp** - Specify that the rule applies to TCP traffic.
  - **src_port_mask** - (Optional) Specify the TCP source port mask.
    - **<hex 0x0-0xffff>** - Enter the source TCP port mask here.
  - **dst_port_mask** - (Optional) Specify the TCP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the destination TCP port mask here.
  - **flag_mask** - (Optional) Specify the TCP flag field mask.
    - **all** - Specify that the TCP flag field mask will be set to all.
    - **urg** - (Optional) Specify that the TCP flag field mask will be set to urg.
    - **ack** - (Optional) Specify that the TCP flag field mask will be set to ack.
    - **psh** - (Optional) Specify that the TCP flag field mask will be set to psh.
    - **rst** - (Optional) Specify that the TCP flag field mask will be set to rst.
    - **syn** - (Optional) Specify that the TCP flag field mask will be set to syn.
    - **fin** - (Optional) Specify that the TCP flag field mask will be set to fin.
- **udp** - (Optional) Specify that the rule applies to UDP traffic.
  - **src_port_mask** - (Optional) Specify the UDP source port mask.
    - **<hex 0x0-0xffff>** - Enter the source UDP port mask here.
  - **dst_port_mask** - (Optional) Specify the UDP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the destination UDP port mask here.
- **protocol_id_mask** - (Optional) Specify that the rule applies to the IP protocol ID traffic.
  - **<hex 0x0-0xff>** - Enter the IP protocol ID mask here.
  - **user_define_mask** - (Optional) Specify that the rule applies to the IP protocol ID and the mask options behind the first 4 bytes of the IP payload.
    - **<hex 0x0-0xffffffff>** - Enter the user-defined IP protocol ID mask here.

packet_content_mask - Specify the frame content mask, there are 5 offsets in maximum could be configured. Each offset presents 16 bytes, the range of mask of frame is 80 bytes (5 offsets) in the first eighty bytes of frame.
- **offset_0-15** - (Optional) Specify that the mask pattern offset of the frame will be between 0

	and 15. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 0 and 15 here. **offset_16-31** - (Optional) Specify that the mask pattern offset of the frame will be between 16 and 31. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 16 and 31 here. **offset_32-47** - (Optional) Specify that the mask pattern offset of the frame will be between 32 and 47. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 32 and 47 here. **offset_48-63** - (Optional) Specify that the mask pattern offset of the frame will be between 48 and 63. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 48 and 63 here. **offset_64-79** - (Optional) Specify that the mask pattern offset of the frame will be between 64 and 79. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 64 and 79 here.
ipv6 - Specify IPv6 filtering mask. **class** - (Optional) Specify the IPv6 class. **flowlabel** - (Optional) Specify the IPv6 flowlabel. **source_ipv6_mask** - (Optional) Specify an IPv6 source submask. **<ipv6mask>** - Enter the IPv6 source submask here. **destination_ipv6_mask** - (Optional) Specify an IPv6 destination submask. **<ipv6mask>** - Enter the IPv6 destination submask here.	

Restrictions

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

Example

To create CPU access list rules:

```
DES-3200-28P:admin#create cpu access_profile profile_id 1 ethernet vlan
source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p
ethernet_type
Command: create cpu access_profile profile_id 1 ethernet vlan source_mac 00-00-
00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type


Success.


DES-3200-28P:admin#create cpu access_profile profile_id 2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create cpu access_profile profile_id 2 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code


Success.


DES-3200-28P:admin#
```

17-2 delete cpu access_profile

Description

This command is used to delete CPU access list rules.

Format

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

Parameters

profile_id - Specify the index of access list profile. **<value 1-5>** - Enter the profile ID value here. This value must be between 1 and 5. **all** – Specify that al the access list profiles will be deleted.

Restrictions

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

Example

To delete CPU access list rules:

```
DES-3200-28P:admin#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3200-28P:admin#
```

17-3 config cpu access_profile

Description

This command is used to configure CPU access list entry.

Format

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

Parameters

profile_id - Specify the index of access list profile. **<value 1-5>** - Enter the profile ID value here. This value must be between 1 and 5.
add - Specify that a profile or a rule will be added.
access_id - Specify the index of access list entry. The range of this value is 1-100.

<value 1-100> - Enter the access ID here. This value must be between 1 and 100.

ethernet - Specify that the profile type will be Ethernet.
- **vlan** - (Optional) Specify the VLAN name used.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
- **vlan_id** - (Optional) Specify the VLAN ID used.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here.
- **source_mac** - (Optional) Specify the source MAC address.
  - **<macaddr>** - Enter the source MAC address used for this configuration here.
- **destination_mac** - (Optional) Specify the destination MAC.
  - **<macaddr>** - Enter the destination MAC address used for this configuration here.
- **802.1p** - (Optional) Specify the value of 802.1p priority tag.
  - **<value 0-7>** - Enter the 802.1p priority tag value here. This value must be between 0 and 7.
- **ethernet_type** - (Optional) Specify the Ethernet type.
  - **<hex 0x0-0xffff>** - Enter the Ethernet type value here.

ip - Specify that the profile type will be IP.
- **vlan** - (Optional) Specify the VLAN name used.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
- **vlan_id** - (Optional) Specify the VLAN ID used.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here.
- **source_ip** - (Optional) Specify an IP source address.
  - **<ipaddr>** - Enter the source IP address used for this configuration here.
- **destination_ip** - (Optional) Specify an IP destination address.
  - **<ipaddr>** - Enter the destination IP address used for this configuration here.
- **dscp** - (Optional) Specify the value of DSCP, the value can be configured 0 to 63.
  - **<value 0-63>** - Enter the DSCP value used here.
- **icmp** - (Optional) Specify that the rule applies to ICMP traffic.
  - **type** - (Optional) Specify that the rule applies to the value of ICMP type traffic.
    - **<value 0-255>** - Enter the ICMP type value here. This value must be between 0 and 255.
  - **code** - (Optional) Specify that the rule applies to the value of ICMP code traffic.
    - **<value 0-255>** - Enter the ICMP code value here. This value must be between 0 and 255.
- **igmp** - (Optional) Specify that the rule applies to IGMP traffic.
  - **type** - (Optional) Specify that the rule applies to the value of IGMP type traffic.
    - **<value 0-255>** - Enter the IGMP type value here. This value must be between 0 and 255.
- **tcp** - (Optional) Specify that the rule applies to TCP traffic.
  - **src_port** - (Optional) Specify that the rule applies the range of TCP source port.
    - **<value 0-65535>** - Enter the source port value here. This value must be between 0 and 65535.
  - **dst_port** - (Optional) Specify the range of TCP destination port range.
    - **<value 0-65535>** - Enter the destination port value here. This value must be between 0 and 65535.
  - **flag** - (Optional) Specify the TCP flag fields .
    - **all** - Specify that the TCP flag field mask will be set to all.
    - **urg** - (Optional) Specify that the TCP flag field mask will be set to urg.
    - **ack** - (Optional) Specify that the TCP flag field mask will be set to ack.
    - **psh** - (Optional) Specify that the TCP flag field mask will be set to psh.
    - **rst** - (Optional) Specify that the TCP flag field mask will be set to rst.
    - **syn** - (Optional) Specify that the TCP flag field mask will be set to syn.
    - **fin** - (Optional) Specify that the TCP flag field mask will be set to fin.
- **udp** - Specify that the rule applies to UDP traffic.
  - **src_port** - (Optional) Specify the range of UDP source port range.
    - **<value 0-65535>** - Enter the source port value here. This value must be between 0 and 65535.
  - **dst_port** - (Optional) Specify the range of UDP destination port mask.
    - **<value 0-65535>** - Enter the destination port value here. This value must be between 0

and 65535. **protocol_id** - Specify that the rule applies to the value of IP protocol ID traffic. **<value 0-255>** - Enter the protocol ID value here. This value must be between 0 and 255. **user_define** - (Optional) Specify that the rule applies to the IP protocol ID and the mask options behind the first 4 bytes of the IP payload. **<hex 0x0-0xffffffff>** - Enter the user-defined IP protocol ID mask here.
packet_content - Specify the frame content pattern, there are 5 offsets in maximum could be configure. Each offset presents 16 bytes, the range of content of frame is 80 bytes(5 offsets) in the first eighty bytes of frame. **offset_0-15** - (Optional) Specify that the mask pattern offset of the frame will be between 0 and 15. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 0 and 15 here. **offset_16-31** - (Optional) Specify that the mask pattern offset of the frame will be between 16 and 31. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 16 and 31 here. **offset_32-47** - (Optional) Specify that the mask pattern offset of the frame will be between 32 and 47. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 32 and 47 here. **offset_48-63** - (Optional) Specify that the mask pattern offset of the frame will be between 48 and 63. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 48 and 63 here. **offset_64-79** - (Optional) Specify that the mask pattern offset of the frame will be between 64 and 79. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 64 and 79 here.
ipv6 - Specify the rule applies to IPv6 fields. **class** - (Optional) Specify the value of IPv6 class. **<value 0-255>** - Enter the IPv6 class value here. This value must be between 0 and 255. **flowlabel** - (Optional) Specify the value of IPv6 flowlabel. **<hex 0x0-0xffff>** - Enter the IPv6 flowlabel here. **source_ipv6** - (Optional) Specify the value of IPv6 source address. **<ipv6addr>** - Enter the IPv6 source address used for this configuration here. **destination_ipv6** - (Optional) Specify the value of IPv6 destination address. **<ipv6addr>** - Enter the IPv6 destination address used for this configuration here.
port - Specify the list of ports to be included in this configuration. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specify that all the ports will be used for this configuration.
permit - Specify the packets that match the access profile are permit by the Switch.
deny - Specify the packets that match the access profile are filtered by the Switch.
time_range - (Optional) Specify name of this time range entry. **<range_name 32>** - Enter the time range here.
delete - Specify to delete a rule from the profile ID entered.
access_id - Specify the index of access list entry. The range of this value is 1-100. **<value 1-100>** - Enter the access ID here. This value must be between 1 and 100.

Restrictions

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

Example

To configure CPU access list entry:

```
DES-3200-28P:admin#config cpu access_profile profile_id 1 add access_id 1 ip
vlan default  source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11
code 32 port 1 deny
Command: config cpu access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1
deny

Success.

DES-3200-28P:admin#
```

17-4 enable cpu interface filtering

Description

This command is used to enable CPU interface filtering control.

Format

enable cpu_interface_filtering

Parameters

None.

Restrictions

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

Example

To enable cpu_interface_filtering:

```
DES-3200-28P:admin#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3200-28P:admin#
```

17-5 disable cpu interface filtering

Description

This command is used to disable CPU interface filtering control.

Format

disable cpu_interface_filtering

Parameters

None.

Restrictions

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

Example

To disable cpu_interface_filtering:

```
DES-3200-28P:admin#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-3200-28P:admin#
```

17-6 show cpu access_profile

Description

This command is used to display current access list table.

Format

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

Parameters

profile_id - (Optional) Specify the index of access list profile. **<value 1-5>** - Enter the profile ID used here. This value must be between 1 and 5.

Restrictions

None.

Example

To display current cpu access list table:

```
DES-3200-28P:admin#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Total Unused Rule Entries : 500
Total Used Rule Entries   : 0

================================================================================
```

```
Profile ID: 1     Type: Ethernet

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

Unused Rule Entries: 100
================================================================================



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

MASK on
    VLAN            : 0xFFF
    Source IP       : 20.0.0.0
    Dest IP         : 10.0.0.0
    DSCP
    ICMP
    Type
    Code

Unused Rule Entries: 100
================================================================================



DES-3200-28P:admin#
```

Chapter 18 Debug Software Command List

debug error_log [dump | clear | upload_toTFTP {<ipaddr> <path_filename 64>}]
debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]
debug output [module <module_list> | all] [buffer | console]
debug config error_reboot [enable | disable]
debug config state [enable | disable]
debug show error_reboot state
debug show status {module <module_list>}

18-1 debug error_log

Description

This command is used to dump, clear or upload the software error log to a TFTP server.

Format

debug error_log [dump | clear | upload_toTFTP {<ipaddr> <path_filename 64>}]

Parameters

dump - Display the debug message of the debug log.
clear - Clear the debug log.
upload_toTFTP - Upload the debug log to a TFTP server specified by IP address. **<ipaddr>** - (Optional) Specify the IPv4 address of the TFTP server. **<path_filename 64>** - (Optional) The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrator-level users can issue this command.

Example

To dump the error log:

```
DES-3200-28P:admin#debug error_log dump
Command: debug error_log dump

********************************************************************************
# debug log: 1
# level: fatal
# clock: 10000ms
# time : 2009/03/11 13:00:00

====================== SOFTWARE FATAL ERROR ======================
Invalid mutex handle : 806D6480

Current TASK : bcmARL.0

------------------------ TASK STACKTRACE -----------------------
->802ACE98
->8018C814
->8028FF44
->8028352C
->801D703C
->8013B8A4
->802AE754
->802A5E0C
```

To clear the error log:

```
DES-3200-28P:admin#debug error_log clear
Command: debug error_log clear

Success.

DES-3200-28P:admin#
```

To upload the error log to TFTP server:

```
DES-3200-28P:admin#debug error_log upload_toTFTP 10.0.0.90 debug-log.txt
Command: debug error_log upload_toTFTP 10.0.0.90 debug-log.txt

Connecting to server.............Done.
Upload error log  ..............Done.

DES-3200-28P:admin#
```

18-2 debug buffer

Description

This command is used to show the debug buffer's state, or dump, clear, or upload the debug buffer to a TFTP server.

Format

debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

Parameters

utilization - Display the debug buffer's state.
dump - Display the debug message in the debug buffer.
clear - Clear the debug buffer.
upload_toTFTP - Upload the debug buffer to a TFTP server specified by IP address. **<ipaddr>** - Specify the IPv4 address of the TFTP server. **<path_filename 64>** - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrator users can issue this command.

Example

To show the debug buffer's state:

```
DES-3200-28P:admin#debug buffer utilization
Command: debug buffer utilization

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

DES-3200-28P:admin#
```

To clear the debug buffer:

```
DES-3200-28P:admin#debug buffer clear
Command: debug buffer clear

Success.

DES-3200-28P:admin#
```

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

```
DES-3200-28P:admin#debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt
Command: debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt

Connecting to server.................. Done.
Upload debug file   .................. Done.

DES-3200-28P:admin#
```

18-3 debug output

Description

This command is used to set a specified module's debug message output to debug buffer or local console. If the user uses the command in a Telnet session, the error message also is output to the local console.

Format

debug output [module <module_list> | all] [buffer | console]

Parameters

module - Specify the module list. **<module_list>** - Enter the module list here. **all** - Control output method of all modules.
buffer - Direct the debug message of the module output to debug buffer(default).
console - Direct the debug message of the module output to local console.

Restrictions

Only Administrator-level users can issue this command.

Example

To set all module debug message outputs to local console:

```
DES-3200-28P:admin#debug output all console
Command: debug output all console

Success.

DES-3200-28P:admin#
```

18-4 debug config error_reboot

Description

This command is used to set if the Switch needs to be rebooted when a fatal error occurs. When the error occurs, the watchdog timer will be disabled by the system first, and then all debug information will be saved in NVRAM. If the error_reboot is enabled, the watchdog shall be enabled after all information is stored into NVRAM.

Format

debug config error_reboot [enable | disable]

Parameters

enable – If enabled, the Switch will reboot when a fatal error happens.
disable – If disabled the Switch will not reboot when a fatal error happens, system will hang-up for debug and enter the debug shell mode for debug.

Restrictions

Only Administrator-level users can issue this command.

Example

To set the Switch to not need a reboot when a fatal error occurs:

```
DES-3200-28P:admin#debug config error_reboot disable
Command: debug config error_reboot disable

Success.

DES-3200-28P:admin#
```

18-5 debug config state

Description

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

Format

debug config state [enable | disable]

Parameters

enable - Enable the debug state. **disable** - Disable the debug state.

Restrictions

Only Administrator-level users can issue this command.

Example

To set the debug state to disabled:

```
DES-3200-28P:admin#debug config state disable
Command: debug config state disable

Success.

DES-3200-28P:admin#
```

18-6 debug show error_reboot state

Description

This command is used to display debug error reboot state.

Format

debug show error_reboot state

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show the debug error reboot state:

```
DES-3200-28P:admin#debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

DES-3200-28P:admin#
```

18-7 debug show status

Description

This command is used to display the debug heanler state and the specified module's debug status.

Format

debug show status {module <module_list>}

Parameters

module – (Optional) Specify the module list. **<module_list>** - Enter the module list.

Restrictions

Only Administrator-level users can issue this command.

Example

To show the specified module's debug state:

```
DES-3200-28P:admin#debug show status module MSTP
Command: debug show status module MSTP

Debug Global State  : Enabled

MSTP                : Disabled

DES-3200-28P:admin#
```

To show the debug state:

```
DES-3200-28P:admin#debug show status
Command: debug show status

Debug Global State  : Enabled

MSTP                : Disabled
IMPB                : Disabled
ERPS                : Disabled

DES-3200-28P:admin#
```

Chapter 19 DHCP Local Relay Command List

config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]
config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]
config dhcp_local_relay option_82 circuit_id [default | vendor1]
config dhcp_local_relay option_82 ports <portlist> policy [replace | drop | keep]
config dhcp_local_relay option_82 remote_id [default | user_define <desc 32>]
enable dhcp_local_relay
disable dhcp_local_relay
show dhcp_local_relay
show dhcp_local_relay option_82 ports {<portlist>}

19-1 config dhcp_local_relay vlan

Description

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

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

Format

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

Parameters

<vlan_name 32> - Specify the VLAN name that the DHCP local relay function will be enabled. This name can be up to 32 characters long.
state - Enable or disable DHCP local relay for specified vlan. **enable** - Specify that the DHCP local relay function will be enabled. **disable** - Specify that the DHCP local relay function will be disabled.

Restrictions

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

Example

To enable DHCP local relay for default VLAN:

```
DES-3200-28P:admin#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DES-3200-28P:admin#
```

19-2 config dhcp_local_relay vlan vlanid

Description

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

Format

config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]

Parameters

vlanid - Specify the VLAN ID that the DHCP local relay function will be enabled. **<vlan_id>** - Enter the VLAN ID used here.
state - Enable or disable DHCP local relay for specified vlan. **enable** - Specify that the DHCP local relay function will be enabled. **disable** - Specify that the DHCP local relay function will be disabled.

Restrictions

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

Example

To enable DHCP local relay for default VLAN:

```
DES-3200-28P:admin#config dhcp_local_relay vlan vlanid 1 state enable
Command: config dhcp_local_relay vlan vlanid 1 state enable

Success.

DES-3200-28P:admin#
```

19-3 config dhcp_local_relay option_82 circuit_id

Description

This command is used to configure the circuit id of DHCP relay agent information option 82 of the switch.

Format

config dhcp_local_relay option_82 circuit_id [default | vendor1]

Parameters

default – Specify the cirecuit id of DHCP relay agent to default.
vendor1 - Specify the cirecuit id of DHCP relay agent to vendor1.

Restrictions

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

Example

To configure the circuit id of DHCP relay agent as default:

```
DES-3200-28P:admin#config dhcp_local_relay option_82 circuit_id default
Command: config dhcp_local_relay option_82 circuit_id default

Success.

DES-3200-28P:admin#
```

19-4 config dhcp_local_relay option_82 ports

Description

This command is used to configure the settings of the specified ports for the policy of the option 82.

Format

config dhcp_local_relay option_82 ports <portlist> policy [replace | drop | keep]

Parameters

<portlist> - Specify a list of ports to be configured.
policy - Specify how to process the packets coming from the client side which have the option 82 field. **replace** - Replace the existing option 82 field in the packet. **drop** - Discard if the packet has the option 82 field. **keep** - Retain the existing option 82 field in the packet.

Restrictions

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

Example

To configure port 1 to 5 for the policy of the option 82:

```
DES-3200-28P:admin#config dhcp_local_relay option_82 ports 1-5 policy keep
Command: config dhcp_local_relay option_82 ports 1-5 policy keep

Success.

DES-3200-28P:admin#
```

19-5 config dhcp_local_relay option_82 remote_id

Description

This command is used to configure the remote ID.

Format

config dhcp_local_relay option_82 remote_id [default | user_define <desc 32>]

Parameters

default - Use the Switch's system MAC address as the remote ID.
user_define - Use user-defined string as the remote ID. **<desc 32>** - Enter the maximum of 32 characters. Space is allowed in the string.

Restrictions

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

Example

To configure the remote ID:

```
DES-3200-28P:admin#config dhcp_local_relay option_82 remote_id user_define D-Lin
k L2Switch
Command: config dhcp_local_relay option_82 remote_id user_define D-Link L2Switch

Success.

DES-3200-28P:admin#
```

19-6 enable dhcp_local_relay

Description

This command is used to globally enable the DHCP local relay function on the Switch.

Format

enable dhcp_local_relay

Parameters

None.

Restrictions

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

Example

To enable the DHCP local relay function:

```
DES-3200-28P:admin#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DES-3200-28P:admin#
```

19-7 disable dhcp_local_relay

Description

This command is used to globally disable the DHCP local relay function on the Switch.

Format

disable dhcp_local_relay

Parameters

None.

Restrictions

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

Example

To disable the DHCP local relay function:

```
DES-3200-28P:admin#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DES-3200-28P:admin#
```

19-8 show dhcp_local_relay

Description

This command is used to display the current DHCP local relay configuration.

Format

show dhcp_local_relay

Parameters

None.

Restrictions

None.

Example

To display local dhcp relay status:

```
DES-3200-28P:admin#show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status         : Disabled
DHCP/BOOTP Local Relay VID List       : 1

DHCP Relay Agent Information Option 82 Circuit ID : Default
DHCP Relay Agent Information Option 82 Remote ID : D-Link L2Switch


DES-3200-28P:admin#
```

19-9 show dhcp_local_relay option_82 ports

Description

This command is used to display the current DHCP local relay option 82 configuration of each port.

Format

show dhcp_local_relay option_82 ports {<portlist>}

Parameters

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

Restrictions

None.

Example

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

```
DES-3200-28P:admin#show dhcp_local_relay option_82 ports 1-5
Command: show dhcp_local_relay option_82 ports 1-5

Port  Option 82
      Policy
----  ---------
1     keep
2     keep
3     keep
4     keep
5     keep


DES-3200-28P:admin#
```

Chapter 20 DHCP Relay Command List

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}
config dhcp_relay add ipif <ipif_name 12> <ipaddr>
config dhcp_relay add vlanid <vlan_id_list> <ipaddr>
config dhcp_relay delete ipif <ipif_name 12> <ipaddr>
config dhcp_relay delete vlanid <vlan_id_list> <ipaddr>
config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep] | remote_id [default | user_define <desc 32>]}
config dhcp_relay option_82 circuit_id [default | vendor1]
enable dhcp_relay
disable dhcp_relay
show dhcp_relay {ipif <ipif_name 12>}
config dhcp_relay option_60 state [enable | disable]
config dhcp_relay option_60 add string <multiword 255> relay <ipaddr> [exact-match | partial-match]
config dhcp_relay option_60 default [relay <ipaddr> | mode [relay | drop]]
config dhcp_relay option_60 delete [string <multiword 255> {relay <ipaddr>} | ipaddress <ipaddr> | all | default {<ipaddr>}]
show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}
config dhcp_relay option_61 state [enable | disable]
config dhcp_relay option_61 add [mac_address <macaddr> | string <multiword 255>] [relay <ipaddr> | drop]
config dhcp_relay option_61 default [relay <ipaddr> | drop]
config dhcp_relay option_61 delete [mac_address <macaddr> | string <multiword 255> | all]
show dhcp_relay option_61

20-1 config dhcp_relay

Description

This command is used to configure the DHCP relay feature of the Switch.

Format

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}

Parameters

hops - (Optional) Specify the maximum number of relay hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4. The DHCP packet will be dropped when the relay hop count in the received packet is equal to or greater than this setting. **<int 1-16>** - Enter the maximum number of relay hops here. This value must be between 1 and 16.
time - (Optional) The time field in the DHCP packet must be equal to or greater than this setting to be relayed by the router. The default value is 0. **<sec 0-65535>** - Enter the relay time here. This value must be between 0 and 65535 seconds.

Restrictions

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

Example

To configure the DHCP relay hops and time parameters:

```
DES-3200-28P:admin#config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DES-3200-28P:admin#
```

20-2 config dhcp_relay add

Description

This command is used to add an IP destination address of the DHCP server for relay of DHCP/BOOTP packets.

Format

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

Parameters

ipif_name - The name of the IP interface which contains the IP address below. **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - The DHCP/BOOTP server IP address.

Restrictions

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

Example

To add a DHCP/BOOTP server to the relay table:

```
DES-3200-28P:admin#config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DES-3200-28P:admin#
```

20-3 config dhcp_relay add vlanid

Description

This command is used to add an IP address as a destination to forward (relay) DHCP/BOOTP packets. If there is an IP interface in the VLAN and it has configured a DHCP server at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets.

Format

config dhcp_relay add vlanid <vlan_id_list> <ipaddr>

Parameters

vlanid - Specify the VLAN ID list used for this configuration. **<vlan_id_list>** - Enter the VLAN ID list used for this configuration here.
<ipaddr> - Enter the DHCP/BOOTP server IP address used here.

Restrictions

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

Example

To add a DHCP/BOOTP server 10.43.21.12 to VLAN 1 to 10:

```
DES-3200-28P:admin#config dhcp_relay add vlanid 1-10 10.43.21.12
Command: config dhcp_relay add vlanid 1-10 10.43.21.12

Success.

DES-3200-28P:admin#
```

To display the DHCP relay status:

```
DES-3200-28P:admin#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status         : Disabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Disabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Circuit ID : Default
DHCP Relay Agent Information Option 82 Remote ID : 00-01-02-03-04-00

Interface    Server 1        Server 2        Server 3        Server 4
------------ --------------- --------------- --------------- ---------------

Server           VLAN ID List
---------------  ------------------------------------------------------------
10.43.21.12      1-10

DES-3200-28P:admin#
```

20-4 config dhcp_relay delete

Description

This command is used to delete one of the IP destination addresses in the Switch's relay table.

Format

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

Parameters

ipif - The name of the IP interface which contains the IP address below. **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - The DHCP/BOOTP server IP address.

Restrictions

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

Example

To delete a DHCP/BOOTP server to the relay table:

```
DES-3200-28P:admin#config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DES-3200-28P:admin#
```

20-5 config dhcp_relay delete vlanid

Description

This command is used to delete an IP address as a destination to forward (relay) DHCP/BOOTP packets.

Format

config dhcp_relay delete vlanid <vlan_id_list> <ipaddr>

Parameters

vlanid - Specify the VLAN ID list used for this configuration. **<vlan_id_list>** - Enter the VLAN ID list used for this configuration here.
<ipaddr> - Enter the DHCP/BOOTP server IP address used here.

Restrictions

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

Example

To delete a DHCP/BOOTP server 10.43.21.12 from VLAN 2 and VLAN 3:

```
DES-3200-28P:admin#config dhcp_relay delete vlanid 2-3 10.43.21.12
Command: config dhcp_relay delete vlanid 2-3 10.43.21.12

Success.

DES-3200-28P:admin#
```

20-6 config dhcp_relay option_82

Description

This command is used to configure the processing of DHCP 82 option for the DHCP relay function.

Format

config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep] | remote_id [default | user_define <desc 32>]}

Parameters

state - (Optional) When the state is enabled, the DHCP packet will be inserted with the option 82 field before being relayed to server. The DHCP packet will be processed based on the behaviour defined in check and policy setting. When the state is disabled, the DHCP packet will be relayed directly to server without further check and processing on the packet. The default setting is disabled. **enable** - Specify that the option 82 processing will be enabled. **disable** - Specify that the option 82 processing will be disabled.
check - (Optional) When the state is enabled, For packet come from client side, the packet should not have the option 82's field. If the packet has this option field, it will be dropped. The default setting is disabled. **enable** - Specify that checking will be enabled. **disable** - Specify that checking will be disabled.
policy - (Optional) Specify the policy used. This option takes effect only when the check status is disabled. The default setting is set to 'replace'. **replace** - Replace the existing option 82 field in the packet. The Switch will use it's own Option 82 value to replace the old Option 82 value in the packet. **drop** - Discard if the packet has the option 82 field. If the packet, that comes from the client side, contains and Option 82 value, then the packet will be dropped. If the packet, that comes from the client side doesn't contain an Option 82 value, then insert it's own Option 82 value into the packet. **keep** - Retain the existing option 82 field in the packet. If the packet, that comes from the client side, contains and Option 82 value, then keep the old Option 82 value. If the packet, that comes from the client side, doesn't contain an Option 82 value, then insert it's own Option 82 value into the packet.
remote_id - (Optional) Specify the content in Remote ID suboption. **default** - Use switch's system MAC address as remote ID. **user_define** - Use user-defined string as remote ID. The space character is allowed in the string. **<desc 32>** - Enter the user defined description here. This value can be up to 32 characters long.

Restrictions

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

Example

To configure dhcp_relay option 82:

```
DES-3200-28P:admin#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DES-3200-28P:admin#config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

DES-3200-28P:admin#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DES-3200-28P:admin#config dhcp_relay option_82 remote_id user_define “D-Link L2
Switch”
Command: config dhcp_relay option_82 remote_id user_define "D-Link L2 Switch"

Success.

DES-3200-28P:admin#
```

20-7 config dhcp_relay option_82 circuit_id

Description

This command is used to configure the circuit id of DHCP relay agent information option 82 of the Switch.

Format

config dhcp_relay option_82 circuit_id [default | vendor1]

Parameters

default – Specify the cirecuit id of DHCP relay agent to default.
vendor1 - Specify the cirecuit id of DHCP relay agent to vendor1.

Restrictions

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

Example

To configure the circuit ID as default:

```
DES-3200-28P:admin#config dhcp_relay option_82 circuit_id default
Command: config dhcp_relay option_82 circuit_id default

Success.

DES-3200-28P:admin#
```

20-8 enable dhcp_relay

Description

This command is used to enable the DHCP relay function on the Switch.

Format

enable dhcp_relay

Parameters

None.

Restrictions

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

Example

To enable the DHCP relay function.

```
DES-3200-28P:admin#enable dhcp_relay
Command: enable dhcp_relay

Success.

DES-3200-28P:admin#
```

20-9 disable dhcp_relay

Description

This command is used to disable the DHCP relay function on the Switch.

Format

disable dhcp_relay

Parameters

None.

Restrictions

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

Example

To disable the DHCP relay function:

```
DES-3200-28P:admin#disable dhcp_relay
Command: disable dhcp_relay

Success.

DES-3200-28P:admin#
```

20-10 show dhcp_relay

Description

This command is used to display the current DHCP relay configuration.

Format

show dhcp_relay {ipif <ipif_name 12>}

Parameters

ipif - (Optional) Specify the IP interface name. **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
If no parameter is specified , the system will display all DHCP relay configuration.

Restrictions

None.

Example

To display DHCP relay configuration:

```
DES-3200-28P:admin#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status         : Enabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 2
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Enabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Circuit ID : Default
DHCP Relay Agent Information Option 82 Remote ID : "D-Link L2 Switch"

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


DES-3200-28P:admin#
```

20-11 config dhcp_relay option_60

Description

This command is used to decide whether DHCP relay will process the DHCP option 60 or not.

When option_60 is enabled, if the packet does not have option 60, then the relay servers cannot be determined based on option 60. The relay servers will be determined based on either option 61 or per IPIF configured servers.

If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored.

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

Format

config dhcp_relay option_60 state [enable | disable]

Parameters

state - Specify that the DHCP relay function should use the option 60 rule to relay the DHCP packets.
enable - Specify that the option 60 rule will be enabled.
disable - Specify that the option 60 rule will be disabled.

Restrictions

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

Example

To configure the state of dhcp_relay option 60:

```
DES-3200-28P:admin#config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success

DES-3200-28P:admin#
```

20-12 config dhcp_relay option_60 add

Description

This command is used to configure the option 60 relay rules. Note that different string can be specified with the same relay server, and the same string can be specified with multiple relay servers.

The system will relay the packet to all the matching servers.

Format

config dhcp_relay option_60 add string <multiword 255> relay <ipaddr> [exact-match | partial-match]

Parameters

string - Specify the string used. **<multiword 255>** - Enter the string value here. This value can be up to 255 characters long.
relay - Specify a relay server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
exact-match - The option 60 string in the packet must full match with the specified string. **partial-match** - The option 60 string in the packet only need partial match with the specified string.

Restrictions

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

Example

To configure the DHCP relay option 60 option:

```
DES-3200-28P:admin#config dhcp_relay option_60 add string "abc" relay
10.90.90.1 exact-match
Command: config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-
match

Success.

DES-3200-28P:admin#
```

20-13 config dhcp_relay option_60 default

Description

This command is used to configure the DHCP relay option 60 default drop option.

When there are no match servers found for the packet based on option 60, the relay servers will be determined by the default relay server setting.

When there is no matching found for the packet, the relay servers will be determined based on the default relay servers.

When drop is specified, the packet with no matching rules found will be dropped without further process.

If the setting is no- drop, then the packet will be processed further based on option 61. The final relay servers will be the union of option 60 default relay servers and the relay servers determined by option 61.

Format

config dhcp_relay option_60 default [relay <ipaddr> | mode [relay | drop]]

Parameters

relay - Specify the IP address used for the DHCP relay forward function. **<ipaddr>** - Enter the IP address used for this configuration here.
mode - Specify the DHCP relay option 60 mode. **relay** - The packet will be relayed based on the relay rules. **drop** - Specify to drop the packet that has no matching option 60 rules.

Restrictions

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

Example

To configure the DHCP relay option 60 default drop option:

```
DES-3200-28P:admin#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

DES-3200-28P:admin#
```

20-14 config dhcp_relay option_60 delete

Description

This command is used to delete DHCP relay option 60 entry.

Format

config dhcp_relay option_60 delete [string <multiword 255> {relay <ipaddr>} | ipaddress <ipaddr> | all | default {<ipaddr>}]

Parameters

string - Delete all the entries whose string is equal to the string of specified if ipaddress is not specified **<multiword 255>** - Enter the DHCP option 60 string to be removed here. This value can be up to 255 characters long.
relay - (Optional) Delete one entry, whose string and IP address are equal to the string and IP address specified by the user. **<ipaddr>** - Enter the IP address used for this configuration here.
ipaddress - Delete all the entry whose ipaddress is equal to the specified ipaddress. **<ipaddr>** - Enter the IP address used for this configuration here. **all** - Delete all the entry. Default relay servers are excluded.
default - Delete the default relay ipaddress that is specified by the user. **<ipaddr>** - (Optional) Enter the IP address used for this configuration here.

Restrictions

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

Example

To delete the DHCP relay option 60 string called ‘abc’:

```
DES-3200-28P:admin#config dhcp_relay option_60 delete string "abc" relay
10.90.90.1
Command: config dhcp_relay option_60 delete string "abc" relay 10.90.90.1

Success.

DES-3200-28P:admin#
```

20-15 show dhcp_relay option_60

Description

This command is used to show DHCP relay option 60 entry by the user specified.

Format

show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}

Parameters

string - (Optional) Show the entry which’s string equal the string of specified. **<multiword 255>** - Enter the entry's string value here. This value can be up to 255 characters long.
ipadddress - (Optional) Show the entry whose IP address equal the specified ipaddress. **<ipaddr>** - Enter the IP address here.
default - (Optional) Show the defaut behaviour of DHCP relay option 60.
If no parameter is specified then all the DHCP option 60 entries will be displayed.

Restrictions

None.

Example

To show DHCP option 60 information:

```
DES-3200-28P:admin#show dhcp_relay option_60
Command: show dhcp_relay option_60

Default Processing Mode: Drop

Default Servers:

Matching Rules:

String                          Match Type            IP Address
-------                         ---------             ---------
abc                             Exact Match           10.90.90.1

Total Entries : 1

DES-3200-28P:admin#
```

20-16 config dhcp_relay option_61

Description

This command is used to decide whether the DHCP relay will process the DHCP option 61 or not.

When option 61 is enabled, if the packet does not have option 61, then the relay servers cannot be determined based on option 61.

If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored.

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

Format

config dhcp_relay option_61 state [enable | disable]

Parameters

state - Specify whether the DHCP relay option 61 is enabled or disabled. **enable** - Enables the function DHCP relay use option 61 ruler to relay DHCP packet. **disable** - Disables the function DHCP relay use option 61 ruler to relay DHCP packet.

Restrictions

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

Example

To configure the state of dhcp_relay option 61:

```
DES-3200-28P:admin#config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success

DES-3200-28P:admin#
```

20-17 config dhcp_relay option_61 add

Description

This command is used to add a rule to determine the relay server based on option 61. The match rule can base on either MAC address or a user-specified string. Only one relay server can be specified for a MAC-address or a string.

If relay servers are determined based on option 60, and one relay server is determined based on option 61, the final relay servers will be the union of these two sets of the servers.

Format

config dhcp_relay option_61 add [mac_address <macaddr> | string <multiword 255>] [relay <ipaddr> | drop]

Parameters

mac_address - The client's client-ID which is the hardware address of client. **<macaddr>** - Enter the client's MAC address here.
string - The client's client-ID, which is specified by administrator. **<multiword 255>** - Enter the client's description here. This value can be up to 255 characters long.
relay - Specify to relay the packet to a IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
drop - Specify to drop the packet.

Restrictions

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

Example

To configure the DHCP relay option 61 function:

```
DES-3200-28P:admin#config dhcp_relay option_61 add mac_address 00-11-22-33-44-
55 drop
Command: config dhcp_relay option_61 add mac_address 00-11-22-33-44-55 drop

Success

DES-3200-28P:admin#
```

20-18 config dhcp_relay option_61 default

Description

This command is used to configure the default ruler for option 61.

Format

config dhcp_relay option_61 default [relay <ipaddr> | drop]

Parameters

relay - Specify to relay the packet that has no option matching 61 matching rules to an IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
drop - Specify to drop the packet that have no option 61 matching rules.

Restrictions

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

Example

To configure the DHCP relay option 61 function:

```
DES-3200-28P:admin#config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success

DES-3200-28P:admin#
```

20-19 config dhcp_relay option_61 delete

Description

This command is used to delete an option 61 rule.

Format

config dhcp_relay option_61 delete [mac_address <macaddr> | string <multiword 255> | all]

Parameters

mac_address - The entry with the specified MAC address will be deleted. **<macaddr>** - Enter the MAC address here.
string - The entry with the specified string will be deleted. **<multiword 255>** - Enter the string value here. This value can be up to 255 characters long.
all - All rules excluding the default rule will be deleted.

Restrictions

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

Example

To remove a DHCP relay option 61 entry:

```
DES-3200-28P:admin#config dhcp_relay option_61 delete mac_address 00-11-22-33-
44-55
Command: config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55


Success


DES-3200-28P:admin#
```

20-20 show dhcp_relay option_61

Description

This command is used to show all rulers for option 61.

Format

show dhcp_relay option_61

Parameters

None.

Restrictions

None.

Example

To display DHCP relay rulers for option 61:

```
DES-3200-28P:admin#show dhcp_relay option_61
Command: show dhcp_relay option_61

Default Relay Rule:Drop

Matching Rules:

Client-ID                     Type               Relay Rule
-----------                   ----               ---------
00-11-22-33-44-55             MAC Address        Drop


Total Entries : 1


DES-3200-28P:admin#
```

Chapter 21 DHCP Server Screening Command List

config filter dhcp_server [add permit server_ip <ipaddr> ports [<portlist> | all] | delete permit server_ip <ipaddr> ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]
show filter dhcp_server

21-1 config filter dhcp_server

Description

This command is used to configure DHCP server screening.

With DHCP server screening function, illegal DHCP server packet will be filtered. This command is used to configure the state of the function for filtering of DHCP server packet and to add/delete the DHCP server binding entry.

This command is useful for projects that support per port control of the DHCP server screening function. The filter can be based on the DHCP server IP address.

The command has two purposes: To specify to filter all DHCP server packets on the specific port and to specify to allow some DHCP server packets with pre-defined server IP addresses. With this function, we can restrict the DHCP server to service specific DHCP clients. This is useful when two DHCP servers are present on the network, one of them provides the private IP address, and one of them provides the IP address.

Enabling filtering of the DHCP server port state will create one access profile and create one access rule per port (UDP port = 67). Filter commands in this file will share the same access profile.

Addition of a permit DHCP entry will create one access profile and create one access rule. Filtering commands in this file will share the same access profile.

Format

config filter dhcp_server [add permit server_ip <ipaddr> ports [<portlist> | all] | delete permit server_ip <ipaddr> ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]

Parameters

add permit server_ip - Specify to add a DHCP permit server IP address. **<ipaddr>** - Enter the DHCP server IP address here. **ports** - The port number of filter DHCP server. **<portlist>** - Enter the list of ports to be configured here. **all** - Specify that all the port will be used for this configuration.
delete permit server_ip - Specify to delete a DHCP permit server IP address. **<ipaddr>** - Enter the DHCP server IP address here. **ports** - The port number of filter DHCP server. **<portlist>** - Enter the list of ports to be configured here. **all** - Specify that all the port will be used for this configuration.

state - Specify the state of the DHCP server filtering. **enable** - Enable the DHCP server filtering. **disable** - Disable the DHCP server filtering.
illegal_server_log_suppress_duration - Specify the same illegal DHCP server IP address detected will be logged only once within the duration. The default value is 5 minutes. **1min** - Specify that illegal server log suppress duration value will be set to 1 minute. **5min** - Specify that illegal server log suppress duration value will be set to 5 minutes. **30min** - Specify that illegal server log suppress duration value will be set to 30 minutes.
trap_log - Specify the trap and log status. **enable** - Enable trap and log status. **disable** - Disable trap and log status.

Restrictions

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

Example

To add an entry from the DHCP server filter list in the Switch's database:

```
DES-3200-28P:admin#config filter dhcp_server add permit server_ip 10.90.90.20
ports 1-20
Command: config filter dhcp_server add permit server_ip 10.90.90.20 ports 1-20

Success.

DES-3200-28P:admin#
```

```
DES-3200-28P:admin#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

DES-3200-28P:admin#
```

21-2 show filter dhcp_server

Description

This command is used to display the DHCP server filter list created on the Switch.

Format

show filter dhcp_server

Parameters

None.

Restrictions

None.

Example

To display the DHCP server/client filter list created on the Switch:

```
DES-3200-28P:admin#show filter dhcp_server
Command: show filter dhcp_server

Enabled Ports: 1-10
Trap & Log State: Disabled
Illegal Server Log Suppress Duration:5 minutes

Permit DHCP Server/Client Table:
Server IP Address Client MAC Address  Port
----------------- ------------------  --------------------
10.90.90.20       All Client MAC      1-20

 Total Entries: 1


DES-3200-28P:admin#
```

Chapter 22 Digital Diagnostic Monitoring (DDM) Commands

config ddm [trap | log] [enable | disable]
config ddm ports [<portlist> | all] [[temperature_threshold | voltage_threshold | bias_current_threshold | tx_power_threshold | rx_power_threshold] {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} | {state[enable|disable] | shutdown [alarm | warning | none]}]
show ddm
show ddm ports {<portlist>} [status | configuration]

22-1 config ddm

Description

The command configures the DDM log and trap action when encountering an exceeding alarm or warning thresholds event.

Format

config ddm [trap | log] [enable | disable]

Parameters

trap - Specify whether to send traps, when the operating parameter exceeds the corresponding threshold. The DDM trap is disabled by default.
log - Specify whether to send a log, when the operating parameter exceeds the corresponding threshold. The DDM log is enabled by default.
enable - Specify to enable the log or trap sending option.
disable - Specify to disable the log or trap sending option.

Restrictions

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

Example

To configure DDM log state to enable:

```
DES-3200-28P:admin#config ddm log enable
Command: config ddm log enable

Success.

DES-3200-28P:admin#
```

To configure DDM trap state to enable:

```
DES-3200-28P:admin#config ddm trap enable
Command: config ddm trap enable

Success.

DES-3200-28P:admin#
```

22-2 config ddm ports

Description

The command is used to configure the DDM settings of the specified ports.

Format

config ddm ports [<portlist> | all] [[temperature_threshold | voltage_threshold | bias_current_threshold | tx_power_threshold | rx_power_threshold] {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} | {state[enable|disable] | shutdown [alarm | warning | none]}]

Parameters

<portlist> - Enter the range of ports to be configured here.
all - Specify that all the optic ports' operating parameters will be configured.
temperature_threshold - Specify the threshold of the optic module's temperature in centigrade. At least one parameter shall be specified for this threshold.
voltage_threshold - Specify the threshold of optic module's voltage.
bias_current_threshold - Specify the threshold of the optic module's bias current.
tx_power_threshold - Specify the threshold of the optic module's output power.
rx_power_threshold - Specify the threshold of optic module's received power.
high_alarm - (Optional) Specify the high threshold for the alarm. When the operating parameter rises above this value, the action associated with the alarm is taken. **<float>** - Enter the high threshold alarm value used here. **low_alarm** - (Optional) Specify the low threshold for the alarm. When the operating parameter falls below this value, the action associated with the alarm is taken. **<float>** - Enter the low threshold alarm value used here. **high_warning** - (Optional) Specify the high threshold for the warning. When the operating parameter rises above this value, the action associated with the warning is taken. **<float>** - Enter the high threshold warning value here. **low_warning** - (Optional) Specify the low threshold for the warning. When the operating parameter falls below this value, the action associated with the warning is taken. **<float>** - Enter the low threshold warning value here.
state - (Optional) Specify the DDM state to enable or disable. If the state is disabled, no DDM action will take effect. **enable** - Specify to enable the DDM state. **disable** - Specify to disable the DDM state.
shutdown - (Optional) Specify whether or not to shutdown the port when the operating parameter exceeds the corresponding alarm threshold or warning threshold. The default value is none. **alarm** - Shutdown the port when the configured alarm threshold range is exceeded. **warning** - Shutdown the port when the configured warning threshold range is exceeded. **none** - The port will never shutdown regardless if the threshold ranges are exceeded or not.

Restrictions

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

Example

To configure the port 25's temperature threshold:

```
DES-3200-28P:admin#config ddm ports 25 temperature_threshold high_alarm 84.9532
low_alarm -10 high_warning 70 low_warning 2.25
Command: config ddm ports 25 temperature_threshold high_alarm 84.9532 low_alarm
-10 high_warning 70 low_warning 2.25

 According to the DDM precision definition, closest value 84.9531 is chosen.

Success.

DES-3200-28P:admin#
```

To configure the port 25's voltage threshold:

```
DES-3200-28P:admin#config ddm ports 25 voltage_threshold high_alarm 4.25
low_alarm 2.5 high_warning 3.5 low_warning 3
Command: config ddm ports 25 voltage_threshold high_alarm 4.25 low_alarm 2.5
high_warning 3.5 low_warning 3

Success.

DES-3200-28P:admin#
```

To configure the port 25's bias current threshold:

```
DES-3810-28:admin#config ddm ports 25 bias_current_threshold high_alarm 7.25
low_alarm 0.004 high_warning 0.5 low_warning 0.008
Command: config ddm ports 25 bias_current_threshold high_alarm 7.25 low_alarm
0.004 high_warning 0.5 low_warning 0.008

Success.

DES-3810-28:admin#
```

To configure the port 25's transmit power threshold:

```
DES-3200-28P:admin#config ddm ports 25 bias_current_threshold high_alarm 7.25
low_alarm 0.004 high_warning 0.5 low_warning 0.008
Command: config ddm ports 25 bias_current_threshold high_alarm 7.25 low_alarm
0.004 high_warning 0.5 low_warning 0.008

Success.

DES-3200-28P:admin#
```

To configure the port 25's receive power threshold:

```
DES-3200-28P:admin#config ddm ports 25 rx_power_threshold high_alarm 4.55
low_alarm 0.01 high_warning 3.5 low_warning 0.03
Command: config ddm ports 25 rx_power_threshold high_alarm 4.55 low_alarm 0.01
high_warning 3.5 low_warning 0.03

Success.

DES-3200-28P:admin#
```

To configure the port 25's actions associate with the alarm:

```
DES-3200-28P:admin#config ddm ports 25 state enable shutdown alarm
Command: config ddm ports 25 state enable shutdown alarm

Success.

DES-3200-28P:admin#
```

22-3 show ddm

Description

This command is used to display the DDM global settings.

Format

show ddm

Parameters

None.

Restrictions

None.

Example

To display the DDM global settings:

```
DES-3200-28P:admin#show ddm
Command: show ddm

DDM Log           :Enabled
DDM Trap          :Disabled



DES-3200-28P:admin#
```

22-4 show ddm ports

Description

This command is used to show the current operating DDM parameters and configuration values of the optic module of the specified ports. There are two types of thresholds: the administrative configuration and the operation configuration threshold.

For the optic port, when a particular threshold was configured by user, it will be shown in this command with a tag indicating that it is a threshold that user configured, else it would be the threshold read from the optic module that is being inserted.

Format

show ddm ports {<portlist>} [status | configuration]

Parameters

<portlist> - (Optional) Enter the range of ports to be displayed here.
status - Specifies that the operating parameter will be displayed.
configuration - Specifies that the configuration values will be displayed.

Restrictions

None.

Example

To display ports 25-26's operating parameters:

```
DES-3200-28P:admin#show ddm ports 25-26 status
Command: show ddm ports 25-26 status

 Port    Temperature   Voltage    Bias Current   TX Power     RX Power
        (in Celsius)     (V)         (mA)         (mW)         (mW)
------- ------------- ---------- -------------- ---------- ------------
  25         -            -            -            -            -
  26         -            -            -            -            -









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

Chapter 23 D-Link Unidirectional Link Detection (DULD) Command List

config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}(1)
show duld ports {<portlist>}

23-1 config duld ports

Description

The command is used to configure unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discovery its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.

Format

config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}(1)

Parameters

<portlist> - Specify a range of ports.
all - Specify to select all ports.
state - Specify these ports unidirectional link detection status. **enable** - Enable unidirectional link detection status. **disable** - Disable unidirectional link detection status.
mode - Specify the mode when detecting unidirectional link. **shutdown** - If any unidirectional link is detected, disable the port and log an event. **normal** - Only log an event when a unidirectional link is detected.
discovery_time - Specify these ports neighbor discovery time. If OAM discovery cannot complete in the discovery time, the unidirectional link detection will start. **<sec 5-65535>** - Enter a time in second. The default discovery time is 5 seconds.

Restrictions

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

Example

To enable unidirectional link detection on port 1:

```
DES-3200-28P:admin#config duld ports 1 state enable
Command: config duld ports 1 state enable

Success.

DES-3200-28P:admin#
```

23-2 show duld ports

Description

This command is used to show unidirectional link detection information.

Format

show duld ports {<portlist>}

Parameters

<portlist> - (Optional) Specify a range of ports.

Restrictions

None.

Example

To show ports 1-4 unidirectional link detection information:

```
DES-3200-28P:admin#show duld ports 1-4
Command: show duld ports 1-4

Port   Admin State  Oper Status  Mode      Link Status     Discovery Time(Sec)
-----  -----------  -----------  --------  --------------  -------------------
1      Enabled      Disabled     Normal    Unknown         5
2      Disabled     Disabled     Normal    Unknown         5
3      Disabled     Disabled     Normal    Unknown         5
4      Disabled     Disabled     Normal    Unknown         5

DES-3200-28P:admin#
```

Chapter 24 DoS Attack Prevention Command List

config dos_prevention dos_type [{land_attack | blat_attack | tcp_null_scan | tcp_xmasscan | tcp_synfin | tcp_syn_srcport_less_1024 | ping_death_attack | tcp_tiny_frag_attack} | all] {action [drop] | state [enable | disable]}
show dos_prevention {land_attack | blat_attack | tcp_null_scan | tcp_xmasscan | tcp_synfin | tcp_syn_srcport_less_1024 | ping_death_attack | tcp_tiny_frag_attack}
config dos_prevention trap [enable | disable]
config dos_prevention log [enable | disable]

24-1 config dos_prevention dos_type

Description

This command is used to configure the prevention of each Denial-of-Service (DoS) attack, including state and action. The packet matching will be done by hardware. For a specific type of attack, the content of the packet will be matched against a specific pattern.

Format

config dos_prevention dos_type [{land_attack | blat_attack | tcp_null_scan | tcp_xmasscan | tcp_synfin | tcp_syn_srcport_less_1024 | ping_death_attack | tcp_tiny_frag_attack} | all] {action [drop] | state [enable | disable]}

Parameters

land_attack - (Optional) Check whether the source address is equal to destination address of a received IP packet.
blat_attack - (Optional) Check whether the source port is equal to destination port of a received TCP packet.
tcp_null_scan - (Optional) Check whether a received TCP packet contains a sequence number of 0 and no flags
tcp_xmasscan - (Optional) Check whether a received TCP packet contains URG, Push and FIN flags.
tcp_synfin - (Optional) Check whether a received TCP packet contains FIN and SYN flags.
tcp_syn_srcport_less_1024 - (Optional) Check whether the TCP packets source ports are less than 1024 packets.
ping_death_attack - (Optional) Detect whether received packets are fragmented ICMP packets.
tcp_tiny_frag_attack - (Optional) Check whether the packets are TCP tiny fragment packets.
all - Specify all DoS attack type.
action – (Optional) When enabling DoS prevention, the following actions can be taken. **drop** – Drop DoS attack packets.
state - (Optional) Specify the DoS attack prevention state. **enable** - Enable DoS attack prevention. **disable** - Disabe DoS attack prevention.

Restrictions

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

Example

To configure land attack and blat attack prevention, the action is drop:

```
DES-3200-28P:admin#config dos_prevention dos_type land_attack blat_attack action
drop state enable
Command: config dos_prevention dos_type land_attack blat_attack action drop
state enable

Success.

DES-3200-28P:admin#
```

24-2 show dos_prevention

Description

This command is used to display DoS prevention information, including the Trap/Log state, the type of DoS attack, the prevention state, the corresponding action if the prevention is enabled and the counter information of the DoS packet.

Format

show dos_prevention {land_attack | blat_attack | tcp_null_scan | tcp_xmasscan | tcp_synfin | tcp_syn_srcport_less_1024 | ping_death_attack | tcp_tiny_frag_attack}

Parameters

land_attack - (Optional) Check whether the source address is equal to destination address of a received IP packet.
blat_attack - (Optional) Check whether the source port is equal to destination port of a received TCP packet.
tcp_null_scan - (Optional) Check whether a received TCP packet contains a sequence number of 0 and no flags
tcp_xmasscan - (Optional) Check whether a received TCP packet contains URG, Push and FIN flags.
tcp_synfin - (Optional) Check whether a received TCP packet contains FIN and SYN flags.
tcp_syn_srcport_less_1024 - (Optional) Check whether the TCP packets source ports are less than 1024 packets.
ping_death_attack - (Optional) Detect whether received packets are fragmented ICMP packets.
tcp_tiny_frag_attack - (Optional) Check whether the packets are TCP tiny fragment packets.

Restrictions

None.

Example

To display DoS prevention information:

```
DES-3200-28P:admin#show dos_prevention
Command: show dos_prevention

Trap:Disabled   Log:Disabled    Function Version  : 1.01

DoS Type                    State     Action            Frame Counts
--------------------------  --------  ----------------  ------------
Land Attack                 Enabled   Drop              -
Blat Attack                 Enabled   Drop              -
TCP Null Scan               Disabled  Drop              -
TCP Xmas Scan               Disabled  Drop              -
TCP SYNFIN                  Disabled  Drop              -
TCP SYN SrcPort Less 1024   Disabled  Drop              -
Ping of Death Attack        Disabled  Drop              -
TCP Tiny Fragment Attack    Disabled  Drop              -



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

24-3 config dos_prevention trap

Description

This command is used to enable or disable DoS prevention trap state.

Format

config dos_prevention trap [enable | disable]

Parameters

enable - Enable DoS prevetion trap state.
disable - Disable DoS prevention trap state.

Restrictions

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

Example

To disable DoS prevention trap:

```
DES-3200-28P:admin#config dos_prevention trap disable
Command: config dos_prevention trap disable

Success.

DES-3200-28P:admin#
```

24-4 config dos_prevention log

Description

This command is used to enable or disable dos prevention log state.

Format

config dos_prevention log [enable | disable]

Parameters

enable - Enable DoS prevetion log state.
disable - Disable DoS prevention log state.

Restrictions

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

Example

To enable DoS prevention log:

```
DES-3200-28P:admin#config dos_prevention log enable
Command: config dos_prevention log enable

Success.

DES-3200-28P:admin#
```

Chapter 25 Ethernet Ring Protection Switching (ERPS) Command List

enable erps
disable erps
create erps raps_vlan <vlanid>
delete erps raps_vlan <vlanid>
config erps raps_vlan <vlanid> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west <port> | east <port>] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add | delete] vlanid <vidlist> | revertive [enable | disable] | timer {holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000> | wtr_time <min 5 - 12>}]
config erps log [enable | disable]
config erps trap [enable | disable]
show erps

25-1 enable erps

Description

This command is used to enable the global ERPS function on a switch. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. The default state is disabled.

The global ERPS function cannot be enabled, when any ERPS ring on the device is enabled and the integrity of any ring parameter is not available. For each ring with the ring state enabled when ERPS is enabled, the following integrity will be checked:

1. R-APS VLAN is created.
2. The Ring port is a tagged member port of the R-APS VLAN.
3. The RPL port is specified if the RPL owner is enabled.
4. The RPL port is not sepcified as virtual channel.

Format

enable erps

Parameters

None.

Restrictions

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

Example

To enable ERPS:

```
DES-3200-28P:admin#enable erps
Command: enable erps

Success.

DES-3200-28P:admin#
```

25-2 disable erps

Description

This command is used to disable the global ERPS function on a switch.

Format

disable erps

Parameters

None.

Restrictions

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

Example

To disable ERPS:

```
DES-3200-28P:admin#disable erps
Command: disable erps

Success.

DES-3200-28P:admin#
```

25-3 create erps raps_vlan

Description

This command is used to create an R-APS VLAN on a switch. Only one R-APS VLAN should be used to transfer R-APS messages.

Note that the R-APS VLAN must already have been created by the create vlan command.

Format

create erps raps_vlan <vlanid>

Parameters

raps_vlan - Specify the VLAN which will be the R-APS VLAN.

<vlanid> - Enter the VLAN ID used here.

Restrictions

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

Example

To create an R-APS VLAN:

```
DES-3200-28P:admin#create erps raps_vlan 4094
Command: create erps raps_vlan 4094

Success.

DES-3200-28P:admin#
```

25-4 delete erps raps_vlan

Description

This command is used to delete an R-APS VLAN on a switch. When an R-APS VLAN is deleted, all parameters related to this R-APS VLAN will also be deleted. This command can only be issued when the ring is not active.

Format

delete erps raps_vlan <vlanid>

Parameters

raps_vlan - Specify the VLAN which will be the R-APS VLAN. **<vlanid>** - Enter the VLAN ID used here.

Restrictions

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

Example

To delete an R-APS VLAN:

```
DES-3200-28P:admin#delete erps raps_vlan 4094
Command: delete erps raps_vlan 4094

Success.

DES-3200-28P:admin#
```

25-5 config erps raps_vlan

Description

This command is used to configure the ERPS R-APS VLAN settings.

The ring MEL is one field in the R-APS PDU. Note that if CFM (Connectivity Fault Management) and ERPS are used at the same time, the R-APS PDU is one of a suite of Ethernet OAM PDU. The behavior for forwarding of R-APS PDU should follow the Ethernet OAM. If the MEL of R-APS PDU is not higher than the level of the MEP with the same VLAN on the ring ports, the R-APS PDU cannot be forwarded on the ring.

Restrictions apply for ports that are included in a link aggregation group. A link aggregation group can be configured as a ring port by specifying the master port of the link aggregation port. Only the master port can be specified as a ring port. If the specified link aggregation group is eliminated, the master port retains its ring port status. If the ring port configured on virtual channel, the ring which the port connects to will be considered as a sub-ring. Note that the ring ports cannot be modified when ERPS is enabled.

RPL port - Specify one of the R-APS VLAN ring ports as the RPL port. To remove an RPL port from an R-APS VLAN, use the none designation for rpl_port.

RPL owner - Specify the node as the RPL owner.

Note that the RPL port and RPL owner cannot be modified when ERPS is enabled; and the virtual channel cannot be configured as RPL. For example, if a ring port is configured on the virtual channel and the ring port is configured as an RPL port, an error message will be display and the configuration will fail.

The R-APS VLAN cannot be the protected VLAN. The protected VLAN can be one that has already been created, or it can be used for a VLAN that has not yet been created.

Holdoff timer - The Holdoff timer is used to filter out intermittent link faults when link failures occur during the protection switching process. When a ring node detects a link failure, it will start the holdoff timer and report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within period of time specified.

Guard timer - Guard timer is used to prevent ring nodes from receiving outdated R-APS messages. This timer is used during the protection switching process after the link failure recovers. When the link node detects the recovery of the link, it will report the link failure recovery event (R-APS PDU with NR flag) and start the guard timer. Before the guard timer expires, all received R-APS messages are ignored by this ring node, except in the case where a burst of three R-APS event messages that indicates the topology of a sub-ring has changed and the node needs to flush FDB are received on the node. In this case the recovered link does not go into a blocking state. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

WTR timer - WTR timer is used to prevent frequent operation of the protection switch due to an intermittent defect. This timer is used during the protection switching process when a link failure recovers. It is only used by the RPL owner. When the RPL owner in protection state receives R-APS PDU with an NR flag, it will start the WTR timer. The RPL owner will block the original

unblocked RPL port and start to send R-APS PDU with an RB flag after the link recovery is confirmed within this period of time.

Revertive mode- When revertive is enabled, the traffic link is restored to the working transport link. When revertive is disabled, the traffic link is allowed to use the RPL, after recovering from a failure.

When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. STP and LBD should be disabled on the ring ports before the specified ring is activated.

The ring cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, RPL owner, are configured. Note that these parameters cannot be changed when the ring is activated.

In order to guarantee correct operation, the following integrity will be checked when the ring is enabled and the global ERPS state is enabled.

1. R-APS VLAN is created.
2. The Ring port is the tagged member port of the R-APS VLAN.
3. The RPL port is specified if RPL owner is enabled.

Format

config erps raps_vlan <vlanid> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west <port> | east <port>] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add | delete] vlanid <vidlist> | revertive [enable | disable] | timer {holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000> | wtr_time <min 5 - 12>}]

Parameters

<vlanid> - Enter the R-APS VLAN ID used.
state - Specify to enable or disable the specified ring. **enable** - Enable the state of the specified ring. **disable** - Disable the state of the specified ring. The default value is disabled.
ring_mel - Specify the ring MEL of the R-APS function. The default ring MEL is 1. **<value 0-7>** - Enter the ring MEL value here. This value should be between 0 and 7.
ring_port - Specify the ring port used. **west** - Specify the port as the west ring port. **<port>** - Enter the port number here. **east** - Specify the port as the east ring port. **<port>** - Enter the port number here.
rpl_port - Specify the RPL port used. **west** - Specify the west ring port as the RPL port. **east** - Specify the east ring port as the RPL port. **none** - No RPL port on this node. By default, the node has no RPL port.
rpl_owner - Specify to enable or disable the RPL owner node. **enable** - Specify the device as an RPL owner node. **disable** - This node is not an RPL owner. By default, the RPS owner is disabled.
protected_vlan - Specify to add or delete the protected VLAN group. **add** - Add VLANs to the protected VLAN group. **delete** - Delete VLANs from the protected VLAN group. **vlanid** - Specify the VLAN ID to be removed or added. **<vidlist>** - Enter the VLAN ID list here.
revertive - Specify the state of the R-APS revertive option. **enable** - Specify that the R-APS revertive option will be enabled.

disable - Specify that the R-APS revertive option will be disabled.
timer - Specify the R-APS timer used. **holdoff_time** - (Optional) Specify the holdoff time of the R-APS function. The default holdoff time is 0 milliseconds. **<millisecond 0-10000>** - Enter the hold off time value here. This value must be in the range of 0 to 10000 millseconds. **guard_time** - (Optional) Specify the guard time of the R-APS function. The default guard time is 500 milliseconds. **<millisecond 10-2000>** - Enter the guard time value here. This value must be in the range of 0 to 2000 millseconds. **wtr_time** - (Optional) Specify the WTR time of the R-APS function. **<min 5-12>** - Enter the WTR time range value here. The range is from 5 to 12 minutes. The default WTR time is 5 minutes.

Restrictions

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

Example

To configure the MEL of the ERPS ring for a specific R-APS VLAN:

```
DES-3200-28P:admin#config erps raps_vlan 4094 ring_mel 2
Command: config erps raps_vlan 4094 ring_mel 2

Success.

DES-3200-28P:admin#
```

To configure the ports of the ERPS ring for a specific R-APS VLAN:

```
DES-3200-28P:admin#config erps raps_vlan 4094 ring_port west 5
Command: config erps raps_vlan 4094 ring_port west 5

Success.

DES-3200-28P:admin#
```

To configure the RPL owner for a specific R-APS VLAN:

```
DES-3200-28P:admin#config erps raps_vlan 4094 rpl_owner enable
Command: config erps raps_vlan 4094 rpl_owner enable

Success.

DES-3200-28P:admin#
```

To configure the protected VLAN for a specific R-APS VLAN:

```
DES-3200-28P:admin#config erps raps_vlan 4094 protected_vlan add vlanid 10-20
Command: config erps raps_vlan 4094 protected_vlan add vlanid 10-20

Success.

DES-3200-28P:admin#
```

To configure the ERPS timers for a specific R-APS VLAN:

```
DES-3200-28P:admin#config erps raps_vlan 4094 timer holdoff_time 100 guard_time
1000 wtr_time 10
Command: config erps raps_vlan 4094 timer holdoff_time 100 guard_time 1000
wtr_time 10

Success.

DES-3200-28P:admin#
```

To configure the ring state of the ERPS:

```
DES-3200-28P:admin#config erps raps_vlan 4094 state enable
Command: config erps raps_vlan 4094 state enable

Success.

DES-3200-28P:admin#
```

25-6 config erps log

Description

This command is used to configure the log state of ERPS events.

Format

config erps log [enable | disable]

Parameters

log - Specify to enable or disable the ERPS log state. **enable** - Enter enable to enable the log state. **disable** - Enter disable to disable the log state. The default value is disabled.

Restrictions

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

Example

To configure the ERPS log state:

```
DES-3200-28P:admin#config erps log enable
Command: config erps log enable

Success.

DES-3200-28P:admin#
```

25-7 config erps trap

Description

This command is used to configure trap state of ERPS events.

Format

config erps trap [enable | disable]

Parameters

trap - Specify to enable or disable the ERPS trap state. **enable** - Enter enable to enable the trap state. **disable** - Enter disable to disable the trap state. The default value is disabled.

Restrictions

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

Example

To configure the trap state of the ERPS:

```
DES-3200-28P:admin#config erps trap enable
Command: config erps trap enable

Success.

DES-3200-28P:admin#
```

25-8 show erps

Description

This command is used to display ERPS configuration and operation information.

The port state of the ring port may be as "Forwarding", "Blocking", "Signal Fail". "Forwarding" indicates that traffic is able to be forwarded. "Blocking" indicates that traffic is blocked by ERPS and a signal failure is not detected on the port. "Signal Fail" indicates that a signal failure is detected on the port and traffic is blocked by ERPS.

The RPL owner administrative state could be configured to "Enabled" or "Disabled". But the RPL owner operational state may be different from the RPL owner administrative state, for example, the RPL owner conflict occurs. "Active" is used to indicate that the RPL owner administrative state is enabled and the device is operated as the active RPL owner. "Inactive" is used to indicate that the RPL owner administrative state is enabled, but the device is operated as the inactive RPL owner.

Format

show erps

Parameters

None.

Restrictions

None.

Example

To display ERPS information:

```
DES-3200-28P:admin#show erps
Command: show erps

 Global Status            : Disabled
 Log Status               : Disabled
 Trap Status              : Disabled
 ----------------------------------
 R-APS VLAN               : 4094
 ERPS Status              : Disabled
 Admin West Port          : 5
 Operational West Port    : 5    (Forwarding)
 Admin East Port          :
 Operational East Port    :
 Admin RPL Port           : None
 Operational RPL Port     : None
 Admin Owner              : Enabled
 Operational Owner        : Enabled
 Protected VLANs          : 10-20
 Ring MEL                 : 2
 Holdoff Time             : 100 milliseconds
 Guard Time               : 1000 milliseconds
 WTR Time                 : 10 minutes
 Revertive mode           : Enabled
 Current Ring State       : -

 ----------------------------------
 Total Rings: 1

DES-3200-28P:admin#
```

Chapter 26 Filter Command List

config filter netbios [<portlist> | all] state [enable | disable]
show filter netbios
config filter extensive_netbios [<portlist> | all] state [enable | disable]
show filter extensive_netbios

26-1 config filter netbios

Description

This command is used to configure the Switch to deny the NETBIOS packets on specific ports.

Format

config filter netbios [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Specify the list of ports used.
all - Specify that all the ports will be used for the configuration.
state- Specify the state of the filter to block the NETBIOS packet. **enable** - Specify that the state will be enabled. **disable** - Specify that the state will be disabled.

Restrictions

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

Example

To configure filter netbios state:

```
DES-3200-28P:admin#config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

DES-3200-28P:admin#
```

26-2 show filter netbios

Description

This command is used to display the NETBIOS filter state on the Switch.

Format

show filter netbios

Parameters

None.

Restrictions

None.

Example

To display the filter netbios list created on the Switch:

```
DES-3200-28P:admin#show filter netbios
Command: show filter netbios

Enabled ports: 1-3

DES-3200-28P:admin#
```

26-3 config filter extensive_netbios

Description

This command is used to configure the Switch to filter NETBIOS packets over 802.3 flame on the specific ports.

Format

config filter extensive_netbios [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter the list of ports used for this configuration here.
all - Specify that all the ports will be used this configuration.
state - Enable or disable the filter to block the NETBIOS packet over 802.3 frame. **enable** - Specify that the filter state will be enabled. **disable** - Specify that the filter state will be disabled.

Restrictions

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

Example

To configure filter extensive netbios state.

```
DES-3200-28P:admin#config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

DES-3200-28P:admin#
```

26-4 show filter extensive_netbios

Description

This command is used to display the extensive netbios state on the Switch.

Format

show filter extensive_netbios

Parameters

None.

Restrictions

None.

Example

To display the extensive_state created on the Switch:

```
DES-3200-28P:admin#show filter extensive_netbios
Command: show filter extensive_netbios

Enabled ports: 1-3

DES-3200-28P:admin#
```

Chapter 27 Filter Database (FDB) Command List

create fdb <vlan_name 32> <macaddr> [port <port> | drop]
create fdb vlanid <vidlist> <macaddr> [port <port> | drop]
create multicast_fdb <vlan_name 32> <macaddr>
config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time <sec 10-1000000>
config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]
delete fdb <vlan_name 32> <macaddr>
clear fdb [vlan <vlan_name 32> | port <port> | all]
show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}
show fdb {[port <port> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time | security]}
show multicast vlan_filtering_mode {[vlanid < vidlist> | vlan <vlan_name 32>]}

27-1 create fdb

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database).

Format

create fdb <vlan_name 32> <macaddr> [port <port> | drop]

Parameters

<vlan_name 32> - Specify a VLAN name associated with a MAC address. The maximum length of the VLAN name is 32 bytes.
<macaddr> - The MAC address to be added to the static forwarding table.
port - The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port. **<port>** - Enter the port number corresponding to the MAC destination address here.
drop - Specify the action drop to be taken.

Restrictions

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

Example

To create a unicast MAC forwarding entry:

```
DES-3200-28P:admin#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DES-3200-28P:admin#
```

To filter a unicast MAC:

```
DES-3200-28P:admin#create fdb default 00-00-00-00-01-02 drop
Command: create fdb default 00-00-00-00-01-02 drop

Success.

DES-3200-28P:admin#
```

27-2 create fdb vlanid

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database).

Format

create fdb vlanid <vidlist> <macaddr> [port <port> | drop]

Parameters

<vidlist> - Specify a VLAN ID associated with a MAC address.
<macaddr> - The MAC address to be added to the static forwarding table.
port - The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port. **<port>** - Enter the port number corresponding to the MAC destination address here.
drop - Specify the action drop to be taken.

Restrictions

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

Example

To create a unicast MAC forwarding entry:

```
DES-3200-28P:admin#create fdb vlanid 1 00-00-00-00-02-02 port 5
Command: create fdb vlanid 1 00-00-00-00-02-02 port 5

Success.

DES-3200-28P:admin#
```

To filter a unicast MAC:

```
DES-3200-28P:admin#create fdb vlanid 1 00-00-00-00-02-02 drop
Command: create fdb vlanid 1 00-00-00-00-02-02 drop

Success.

DES-3200-28P:admin#
```

27-3 create multicast_fdb

Description

This command is used to create a static entry in the multicast MAC address forwarding table (database).

Format

create multicast_fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - The name of the VLAN on which the MAC address resides. The maximum name length is 32.
<macaddr> - The multicasts MAC address to be added to the static forwarding table.

Restrictions

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

Example

To create a multicast MAC forwarding entry to the default VLAN:

```
DES-3200-28P:admin#create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DES-3200-28P:admin#
```

27-4 config multicast_fdb

Description

This command is used to configure the Switch's multicast MAC address forwarding database.

Format

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

Parameters

<vlan_name 32> - The name of the VLAN on which the MAC address resides. The maximum

name length is 32.
<macaddr> - The MAC address that will be added or deleted to the forwarding table.
add - Specify to add ports to the multicast forwarding table.
delete - Specify to remove ports from the multicast forwarding table.
<portlist> - Specify a range of ports to be configured.

Restrictions

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

Example

To add a multicast MAC forwarding entry to the default VLAN on port 1 to 5:

```
DES-3200-28P:admin#config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5

Success.

DES-3200-28P:admin#
```

27-5 config fdb aging_time

Description

This command is used to configure the MAC address table aging time.

Format

config fdb aging_time <sec 10-1000000>

Parameters

aging_time - Specify the FDB age out time in seconds. The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 10 to 1000000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the Switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a switch..
<sec 10-1000000> - The FDB age out time must be between 10 to 1000000 seconds.

Restrictions

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

Example

To configure the MAC address table aging time to 600 seconds:

```
DES-3200-28P:admin#config fdb aging_time 600
Command: config fdb aging_time 600

Success.

DES-3200-28P:admin#
```

27-6 config multicast vlan_filtering_mode

Description

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

The registered group will be forwarded to the range of ports in the multicast forwarding database.

Format

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

Parameters

vlanid - Specify a list of VLANs to be configured. **<vidlist>** - Enter the VLAN ID list here.
vlan - Specify the name of the VLAN. The maximum name length is 32. **<vlan_name 32>** - The VLAN name can be up to 32 characters long.
all - Specify all configured VLANs.
forward_all_groups - Both the registered group and the unregistered group will be forwarded to all member ports of the specified VLAN where the multicast traffic comes in.
forward_unregistered_groups - The unregistered group will be forwarded to all member ports of the VLAN where the multicast traffic comes in.
filter_unregistered_groups - The unregistered group will be filtered.

Restrictions

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

Example

To configure the multicast packet filtering mode to filter all unregistered multicast groups for the VLAN 200 to 300:

```
DES-3200-28P:admin#config multicast vlan_filtering_mode vlanid 200-300
filter_unregistered_groups
Command: config multicast vlan_filtering_mode vlanid 200-300
filter_unregistered_groups

Success.

DES-3200-28P:admin#
```

27-7 delete fdb

Description

This command is used to delete a static entry from the forwarding database.

Format

delete fdb <vlan_name 32> <macaddr>

Parameters

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

Restrictions

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

Example

To delete a static FDB entry:

```
DES-3200-28P:admin#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3200-28P:admin#
```

27-8 clear fdb

Description

This command is used to clear the Switch's forwarding database for dynamically learned MAC addresses.

Format

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

Parameters

vlan - Clears the FDB entry by specifying the VLAN name. **<vlan_name 32>** - The name of the VLAN on which the MAC address resides. The maximum name length is 32.
port - Clears the FDB entry by specifying the port number. **<port>** - The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.
all - Clears all dynamic entries in the Switch's forwarding database.

Restrictions

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

Example

To clear all FDB dynamic entries:

```
DES-3200-28P:admin#clear fdb all
Command: clear fdb all

Success.

DES-3200-28P:admin#
```

27-9 show multicast_fdb

Description

This command is used to display the multicast forwarding database of the Switch.

Format

show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}

Parameters

vlan - (Optional) The name of the VLAN on which the MAC address resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Displays the entries for the VLANs indicated by VID list. **<vidlist>** - Enter the VLAN ID list here.
mac_address - (Optional) Specify a MAC address, for which FDB entries will be displayed. **<macaddr>** - Enter the MAC address here.
If no parameter is specified, all multicast FDB entries will be displayed.

Restrictions

None.

Example

To display the multicast MAC address table:

```
DES-3200-28P:admin#show multicast_fdb
Command: show multicast_fdb


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


Total Entries: 1


DES-3200-28P:admin#
```

27-10 show fdb

Description

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

Format

show fdb {[port <port> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time | security]}

Parameters

port - (Optional) Displays the entries for a specified port. **<port>** - Enter the port number here.
vlan - (Optional) Displays the entries for a specific VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Displays the entries for the VLANs indicated by VID list. **<vidlist>** - Enter the VLAN ID list here.
mac_address - (Optional) Displays a specific MAC address. **<macaddr>** - Enter the MAC address here.
static - (Optional) Displays all permanent entries.
aging_time - (Optional) Displays the unicast MAC address aging time.
security - (Optional) Displays the FDB entries that are created by the security module.
If no parameter is specified, system will display the unicast address table.

Restrictions

None.

Example

To display the FDB table:

```
DES-3200-28P:admin#show fdb
Command: show fdb

 Unicast MAC Address Aging Time  = 300

 VID  VLAN Name                         MAC Address       Port  Type    Status
 ---- -------------------------------- ----------------- ----- ------- -------
 1    default                          00-01-02-03-04-00 CPU   Self    Forward
 1    default                          00-23-7D-BC-08-44 1     Dynamic Forward
 1    default                          00-23-7D-BC-2E-18 1     Dynamic Forward
 1    default                          00-26-5A-AE-CA-1C 1     Dynamic Forward
 1    default                          60-33-4B-C4-52-1A 1     Dynamic Forward

Total Entries: 5

DES-3200-28P:admin#
```

To display the security FDB table:

```
DES-3200-28P:admin#show fdb security
Command: show fdb security


VID  MAC Address         Port   Type    Status   Security Module
---- ----------------   ----- ------- -------- ---------------
1    00-00-00-10-00-01  1    Dynamic  Drop      802.1X
1    00-00-00-10-00-02  2    Static   Forward   WAC
1    00-00-00-10-00-04  4    Static   Forward   Port Security
1    00-00-00-10-00-0A  5    Static   Forward   MAC-based Access Control
1    00-00-00-10-00-06  6    Dynamic  Drop       Compound Authentication
Total Entries: 5

DES-3200-28P:admin#
```

27-11 show multicast vlan_filtering_mode

Description

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

Note: A product supports the multicast VLAN filtering mode could not support the port filtering mode at the same time.

Format

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

Parameters

vlanid - (Optional) Specify a list of VLANs to be configured. **<vidlist>** - Enter the VLAN ID list here.
vlan - (Optional) Specify the name of the VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters

long.
If no parameter is specified, the device will show all multicast filtering settings in the device.

Restrictions

None.

Example

To show the multicast vlan_filtering_mode for VLANs:

```
DES-3200-28P:admin#show multicast vlan_filtering_mode
Command: show multicast vlan_filtering_mode

VLAN ID/VLAN Name                          Multicast Filter Mode
-----------------------------------------  ----------------------------
1   /default                               forward_unregistered_groups

DES-3200-28P:admin#
```

Chapter 28 Flash File System (FFS) Command List

show storage_media_info
md {<drive_id>} <pathname>
rd {<drive_id>} <pathname>
cd {<pathname>}
dir {<drive_id>} {<pathname>}
rename {<drive_id>} <pathname> <filename>
del {<drive_id>} <pathname> {recursive}
erase {<drive_id>} <pathname>
move {<drive_id>} <pathname> {<drive_id>} <pathname>
copy {<drive_id>} <pathname> {<drive_id>} <pathname>

28-1 show storage_media_info

Description

This command is used to display the information of the storage media available on the system. The information for a media includes the drive number, the media identification.

Format

show storage_media_info

Parameters

None.

Restrictions

None.

Example

To display the storage media's information:

```
DES-3200-28P:admin#show storage_media_info
Command: show storage_media_info

Drive  Media Type      Size  Label        FS Type
-----  ----------  --------  -----------  -------
c:/    Flash          28 MB               FFS

DES-3200-28P:admin#
```

28-2 md

Description

This command is used to create a directory.

Format

md {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.
<pathname> - Specify the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory. The drive ID also included in this parameter, for example, c:/config/bootup.cfg.

Restrictions

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

Example

To make a directory:

```
DES-3200-28P:admin#md c:/abc
Command: md c:/abc

Success.

DES-3200-28P:admin#
```

28-3 rd

Description

This command is used to remove a directory. If there are files still existing in the directory, this command will fail and return error message.

Format

rd {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.
<pathname> - Specify the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

Restrictions

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

Example

To remove a directory:

```
DES-3200-28P:admin#rd c:/abc
Command: rd c:/abc

Success.

DES-3200-28P:admin#
```

28-4 cd

Description

This command is used to change the current directory. The current directory is changed under the current drive. If you want to change the working directory to the directory in another drive, then you need to change the current drive to the desired drive, and then change the current directory. The current drive and current directory will be displayed if the <pathname> is not specified.

Format

cd {<pathname>}

Parameters

<pathname> - (Optional) Specify the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

Restrictions

None.

Example

To change to other directory or display current directory path:

```
DES-3200-28P:admin#cd
Command: cd

Current work directory: "/c:".

DES-3200-28P:admin#
```

28-5 dir

Description

This command is used to list all the files located in a directory of a drive.

If pathname is not specified, then all of the files in the specified drive will be displayed. If none of the parameters are specified, the files in the current drive will be displayed.

Format

dir {<drive_id>} {<pathname>}

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.
<pathname> - (Optional) Specify the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

Restrictions

None.

Example

List the files:

```
DES-3200-28P:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 RUN(*)  -rw- 5491536  2000/01/01 00:41:03 DES3200_RUNTIME_V4.00.014.had
  2 CFG(*)  -rw- 31142    2000/01/01 02:19:40 config.cfg
  3         d---          2000/01/01 00:00:16 system

29618 KB total (24127 KB free)
(*) -with boot up info          (b) -with backup info

DES-3200-28P:admin#
```

28-6 rename

Description

This command is used to rename a file. Note that for standalone device, the unit argument is not needed. This command is used to rename a file in the file system. The pathname specifies the file (in path form) to be renamed and the filename specifies the new filename. If the pathname is not a full path, then it refers to a path under the current directory for the drive. The renamed file will stay in the same directory.

Format

rename {<drive_id>} <pathname> <filename>

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.
<pathname> - Specify the file (in path form) to be renamed.
<filename> - Specify the new name of the file.

Restrictions

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

Example

To rename a file:

```
DES-3200-28P:admin#rename run.had run1.had
Command: rename run.had run1.had

Success.

DES-3200-28P:admin#
```

28-7 del

Description

This command is used to delete a file, either physically or softly. It is also used to delete a directory and its contents. If two files with the same name under the same directory are softly deleted sequentially, only the last one will exist. Deleting, copying, renaming or moving the already softly deleted file is not acceptable.

System will prompt if the target file is a FW or configuration whose type is bootup.

Format

del {<drive_id>} <pathname> {recursive}

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.
<pathname>- Specify the file or directory to be deleted. If it is specified in the associated form, then it is related to the current directory.
recursive - (Optional) Used on directory, to delete a directory and its contents even if it's not empty.

Restrictions

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

Example

Delete a directory with parameter "recursive":

```
DES-3200-28P:admin#dir
Command: dir

Directory of / c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1         drw- 0        2000/04/02 06:02:04 12
  2 CFG(*)  -rw- 29661    2000/04/01 05:54:38 config.cfg
  3 RUN(*)  -rw- 4879040  2000/03/26 03:15:11 B019.had
  4         d--- 0        2000/04/01 05:17:36 system

29618 KB total (24727 KB free)
(*) -with boot up info          (b) -with backup info

DES-3200-28P:admin#del 12 recursive
Command: del 12 recursive

Success.

DES-3200-28P:admin#dir
Command: dir

Directory of / c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 29661    2000/04/01 05:54:38 config.cfg
  2 RUN(*)  -rw- 4879040  2000/03/26 03:15:11 B019.had
  3         d--- 0        2000/04/01 05:17:36 system

29618 KB total (24727 KB free)
(*) -with boot up info          (b) -with backup info

DES-3200-28P:admin#
```

28-8 erase

Description

This command is used to delete a file stored in the file system.

System will prompt if the target file is a FW or configuration whose type is boot up.

Format

erase {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.
<pathname> - Specify the file to be deleted. If it is specified in the associated form, then it is

related to the current directory.

Restrictions

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

Example

To erase a file:

```
DES-3200-28P:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(b)  -rw- 29661    2000/04/02 06:03:19 config2.cfg
  2 CFG(*)  -rw- 29661    2000/04/01 05:54:38 config.cfg
  3 RUN(*)  -rw- 4879040  2000/03/26 03:15:11 B019.had
  4         d--- 0        2000/04/01 05:17:36 system

29618 KB total (24697 KB free)
(*) -with boot up info          (b) -with backup info

DES-3200-28P:admin#erase config2.cfg
Command: erase config2.cfg

Success.

DES-3200-28P:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 29661    2000/04/01 05:54:38 config.cfg
  2 RUN(*)  -rw- 4879040  2000/03/26 03:15:11 B019.had
  3         d--- 0        2000/04/01 05:17:36 system

29618 KB total (24727 KB free)
(*) -with boot up info          (b) -with backup info

DES-3200-28P:admin#
```

28-9 move

Description

This command is used to move a file around the file system. Note that when a file is moved, it can be specified whether to rename at the same time.

Format

move {<drive_id>} <pathname> {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID, for example, C:.
<pathname> - Specify the file to be moved. The path name can be specified either as a full path name or partial name. Specify either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.
<drive_id> - (Optional) Enter the drive ID, for example, C:.
<pathname> - Specify the new path where the file will be moved. The path name can be. For partial path name, it indicates the file is in the current directory.

Restrictions

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

Example

To move a file from one location to another location:

```
DES-3200-28P:admin#move c:/log.txt c:/log1.txt
Command: move c:/log.txt c:/log1.txt

Success.

DES-3200-28P:admin#
```

28-10 copy

Description

This command is used to copy a file to another file in the file system.

Format

copy {<drive_id>} <pathname> {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID, for example, C:.
<pathname> - Specify the file to be copied. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.
<drive_id> - (Optional) Enter the drive ID, for example, C:.
<pathname> - Specify the file to copy to. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

Restrictions

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

Example

To copy a file:

```
DES-3200-28P:admin#copy c:/log.txt c:/log1.txt
Command: copy c:/log.txt c:/log1.txt

Success.

DES-3200-28P:admin#
```

Chapter 29 Gratuitous ARP Command List

config gratuitous_arp send ipif_status_up [enable | disable]
config gratuitous_arp send dup_ip_detected [enable | disable]
config gratuitous_arp learning [enable | disable]
config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>
enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)
disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)
show gratuitous_arp {ipif <ipif_name 12>}

29-1 config gratuitous_arp send ipif_status_up

Description

The command is used to enable/disable sending of gratuitous ARP request packet while IPIF interface become up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is enabled, and only one gratuitous ARP packet will be broadcast.

Format

config gratuitous_arp send ipif_status_up [enable | disable]

Parameters

enable - Enable sending of gratuitous ARP when IPIF status become up.
disable - Disable sending of gratuitous ARP when IPIF status become up.

Restrictions

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

Example

To enable send gratuitous ARP request in normal situation:

```
DES-3200-28P:admin#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DES-3200-28P:admin#
```

29-2 config gratuitous_arp send dup_ip_detected

Description

The command is used to enable/disable sending of gratuitous ARP request packet while duplicate IP is detected. By default, the state is enabled.For this command, the duplicate IP detected means

that the system received a ARP request packet that is sent by an IP address that match the system's own IP address. In this case, the system knows that some body out there uses an IP address that is conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.

Format

config gratuitous_arp send dup_ip_detected [enable | disable]

Parameters

enable - Enable sending of gratuitous ARP when duplicate IP is detected.
disable - Disable sending of gratuitous ARP when duplicate IP is detected.

Restrictions

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

Example

To enable send gratuitous ARP request when duplicate IP is detected:

```
DES-3200-28P:admin#config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

DES-3200-28P:admin#
```

29-3 config gratuitous_arp learning

Description

This command is used to configure gratuitous ARP learning. Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. The command is used to enable/disable learning of ARP entry in ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for. Note that, with the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet. By default, the state is enabled status.

Format

config gratuitous_arp learning [enable | disable]

Parameters

enable - Enable learning of ARP entry based on the received gratuitous ARP packet.
disable - Disable learning of ARP entry based on the received gratuitous ARP packet.

Restrictions

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

Example

To show the global GratuitousARP state:

```
DES-3200-28P:admin#config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DES-3200-28P:admin#
```

29-4 config gratuitous_arp send periodically

Description

The command is used to configure the interval for periodical sending of gratuitous ARP request packet. By default, the interval is 0.

Format

config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>

Parameters

ipif - Interface name of L3 interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
interval - Periodically send gratuitous ARP interval time in seconds. 0 means not send gratuitous ARP periodically. **<value 0-65535>** - Enter the gratuitous ARP interval time here. This value must be between 0 and 65535 seconds.

Restrictions

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

Example

To configure gratuitous ARP interval to 5 for IPIF System:

```
DES-3200-28P:admin#config gratuitous_arp send periodically ipif System interval
5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DES-3200-28P:admin#
```

29-5 enable gratuitous_arp

Description

The command is used to enable gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.

Format

enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

Parameters

ipif - (Optional) Interface name of L3 interface **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
trap - Specify to enable the trap function.
log - Specify to enable the log function.

Restrictions

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

Example

To enable system interface's gratuitous ARP log and trap:

```
DES-3200-28P:admin#enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

DES-3200-28P:admin#
```

29-6 disable gratuitous_arp

Description

The command is used to disable gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.

Format

disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

Parameters

ipif - (Optional) Interface name of L3 interface **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
trap - Specify to disable the trap function.
log - Specify to disable the log function.

Restrictions

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

Example

To disable system interface's gratuitous ARP log and trap:

```
DES-3200-28P:admin#disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

DES-3200-28P:admin#
```

29-7 show gratuitous_arp

Description

This command is used to display gratuitous ARP configuration.

Format

show gratuitous_arp {ipif <ipif_name 12>}

Parameters

ipif - (Optional) Interface name of L3 interface. **<ipif_name>** - Enter the IP interface name here.

Restrictions

None.

Example

To display gratuitous ARP log and trap state:

```
DES-3200-28P:admin#show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF Status Up        : Enabled
Send on Duplicate IP Detected : Enabled
Gratuitous ARP Learning       : Enabled

IP Interface Name : System
        Gratuitous ARP Trap                     : Enabled
        Gratuitous ARP Log                      : Enabled
        Gratuitous ARP Periodical Send Interval : 5

Total Entries: 1


DES-3200-28P:admin#
```

Chapter 30 IGMP / MLD Snooping Command List

The Internet Group Management Protocol (IGMP) is a L3 protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. IGMP snooping is the process of listening to IGMP network traffic. IGMP snooping, as implied by the name, is a feature that allows a layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyzes all IGMP packets between hosts connected to the Switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the Switch adds the host's port number to the multicast list for that group. And, when the Switch hears an IGMP Leave, it removes the host's port from the table entry.

The Multicast Listener Discovery (MLD) is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3.

The Switch only supports IGMP and MLD snooping awareness. This means that the multicast traffic forwarding is only based on L2 MAC addresses associated to groups that the Switch has joined. The source IP address of the multicast traffic will be ignored.

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable|disable] | report_suppression [enable | disable]
config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)
config igmp access_authentication ports [all | <portlist>] state [enable | disable]
config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable igmp_snooping
disable igmp_snooping
create igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
delete igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>
show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}
config igmp_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}
config igmp_snooping data_driven_learning max_learned_entry <value 1-1024>
clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr> | all]]

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]
show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}
show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
show igmp_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]
show igmp access_authentication ports [all | <portlist>]
clear igmp_snooping statistics counter
config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | report_suppression [enable | disable]
config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)
config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable mld_snooping
disable mld_snooping
show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}} {data_driven}
show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>
show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}
config mld_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)
config mld_snooping data_driven_learning max_learned_entry <value 1-1024>
clear mld_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipv6addr>| all]]
show mld_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]
clear mld_snooping statistics counter
config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

30-1 config igmp_snooping

Description

This command is used to configure IGMP snooping on the Switch.

Format

config igmp_snooping [vlan_name <vlan_name 32> \| vlanid <vlanid_list> \| all] {state [enable \| disable] \| fast_leave [enable|disable] \| report_suppression [enable \| disable]

Parameters

vlan_name - Specify the name of the VLAN for which IGMP snooping is to be configured. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the VLAN ID for which IGMP snooping is to be configured. **<vlanid_list>** - Enter the VLAN ID here.
all - Specify to use all configured VLANs.
state - (Optional) Enable or disable IGMP snooping for the chosen VLAN. **enable** - Enter enable to enable IGMP snooping for the chosen VLAN. **disable** - Enter disable to disable IGMP snooping for the chosen VLAN.
fast_leave - Enable or disable the IGMP snooping fast leave function. **enable** - Enter enable to enable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message. **disable** - Enter disable to disable the IGMP snooping fast leave function.
report_suppression - Specify IGMP report suppression. When enabled, multiple IGMP reports or leave for a specific (S, G) will be integrated into one report only before sending to the router port. **enable** - Enable the IGMP report suppression. **disable** - Disable the IGMP report suppression.

Restrictions

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

Example

To configure IGMP snooping:

```
DES-3200-28P:admin#config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

DES-3200-28P:admin#
```

30-2 config igmp_snooping rate_limit

Description

This command is used to configure the rate of IGMP control packet that is allowed per port or per VLAN.

Format

config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Parameters

ports - Specify a range of ports to be configured. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specify a range of VLANs to be configured. **<vlanid_list>** - Enter the VLAN ID list here.

<value 1-1000> - Configure the rate of the IGMP control packet that the Switch can process on a specific port/VLAN. The rate is specified in packets per second. The packets that exceed the limit will be dropped.
no_limit - Configure the rate of the IGMP control packet to be unlimited that the Switch can process on a specific port/VLAN. The rate is specified in packets per second. The packets that exceed the limit will be dropped. The default setting is no_limit.

Restrictions

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

Example

To configure the IGMP snooping per port rate_limit:

```
DES-3200-28P:admin#config igmp_snooping rate_limit ports 1 100
Command: config igmp_snooping rate_limit ports 1 100

Success.

DES-3200-28P:admin#
```

30-3 config igmp_snooping querier

Description

This command is used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, and the permitted packet loss that guarantees IGMP snooping.

Format

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)

Parameters

vlan_name - Specify the name of the VLAN for which IGMP snooping querier is to be configured.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the VLAN ID for which IGMP snooping querier is to be configured.
<vlanid_list> - Enter the VLAN ID list here.
all - Specify all VLANs for which IGMP snooping querier is to be configured.

query_interval - (Optional) Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds.
<sec 1-65535> - Enter the query interval value here. This value must between between 1 and 65535 seconds.

max_reponse_time - (Optional) Specify the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.
<sec 1-25> - Enter the maximum response time value here. This value must be between 1 and 25 seconds.

robustness_variable - (Optional) Provides fine-tuning to allow for expected packet loss on a

subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: **<value 1-7>** - Enter the robustness variable value here. This value must be between 1 and 7. By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be more loose. • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.
last_member_query_interval - (Optional) Specify the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. On receiving a leave message, the router will assume there are no local members on the interface if there are no reports received after the response time (which is last member query interval * robustness variable) **<sec 1-25>** - Enter the last member query interval value here. This value must be between 1 and 25 seconds.
state - (Optional) If the state is enabled, it allows the Switch to be selected as an IGMP Querier (sends IGMP query packets). It the state is disabled, then the Switch cannot play the role as a querier. Note that if the Layer 3 router connected to the Switch provide only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not send the multicast-routing protocol packet, the port will be timed out as a router port. **enable** - Enter enable to enable this state. **disable** - Enter disable to disable this state.
version - (Optional) Specify the version of IGMP packet that will be sent by this device. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped. **<value 1-3>** - Enter the version number here. This value must be between 1 and 3.

Restrictions

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

Example

To configure the IGMP snooping querier:

```
DES-3200-28P:admin#config igmp_snooping querier vlan_name default
query_interval 125 state enable

Command: config igmp_snooping querier vlan_name default query_interval 125
state enable


Success.


DES-3200-28P:admin#
```

30-4 config igmp access_authentication ports

Description

This command is used to enable or disable the IGMP Access Control function for the specified ports. If the IGMP Access Control function is enabled and the Switch receives an IGMP JOIN message, the Switch will send the access request to the RADIUS server for authentication.

Format

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

Parameters

all - Specify all ports to be configured.
<portlist> - Specify a range of ports to be configured.
state - Specify the state of the RADIUS authentication function on the specified ports. enable - Enable the RADIUS authentication function on the specified ports. disable - Disable the RADIUS authentication function on the specified ports.

Restrictions

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

Example

To enable IGMP Access Control for all ports:

```
DES-3200-28P:admin#config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable

Success.

DES-3200-28P:admin#
```

30-5 config router_ports

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol, etc.

Format

config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

<vlan_name 32> - Specify the name of the VLAN on which the router port resides. **vlanid** - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID here.
add - Specify to add the router ports.

delete - Specify to delete the router ports.
<portlist> - Specify a range of ports to be configured.

Restrictions

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

Example

To set up static router ports:

```
DES-3200-28P:admin#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DES-3200-28P:admin#
```

30-6 config router_ports_forbidden

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Format

config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

<vlan_name 32> - Specify the name of the VLAN on which the router port resides. **vlanid** - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specify to add the router ports. **delete** - Specify to delete the router ports.
<portlist> - Specify a range of ports to be configured.

Restrictions

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

Example

To set up port range 1-10 to forbidden router ports of default VLAN:

```
DES-3200-28P:admin#config router_ports_forbidden default add 11-12
Command: config router_ports_forbidden default add 11-12

Success.

DES-3200-28P:admin#
```

30-7 enable igmp_snooping

Description

This command is used to enable IGMP snooping on the Switch.

Format

enable igmp_snooping

Parameters

None.

Restrictions

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

Example

To enable IGMP snooping on the Switch:

```
DES-3200-28P:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3200-28P:admin#
```

30-8 disable igmp_snooping

Description

This command is used to disable IGMP snooping on the Switch. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.

Format

disable igmp_snooping

Parameters

None.

Restrictions

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

Example

To disable IGMP snooping on the Switch:

```
DES-3200-28P:admin#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3200-28P:admin#
```

30-9 create igmp_snooping static_group

Description

This command is used to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group.

The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports.

The static member port will only affect V2 IGMP operation.

The Reserved IP multicast address 224.0.0.X must be excluded from the configured group.

The VLAN must be created first before a static group can be created.

Format

create igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Parameters

vlan - Specify the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long. **vlanid** - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specify the multicast group IP address.

Restrictions

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

Example

To create an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DES-3200-28P:admin#create igmp_snooping static_group vlan default 239.1.1.1
Command: create igmp_snooping static_group vlan default 239.1.1.1

Success.

DES-3200-28P:admin#
```

30-10 delete igmp_snooping static_group

Description

This command is used to delete an IGMP snooping multicast static group. The deletion of an IGMP snooping static group will not affect the IGMP snooping dynamic member ports for a group.

Format

delete igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Parameters

vlan - Specify the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipaddr> - Specify the multicast group IP address.

Restrictions

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

Example

To delete an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DES-3200-28P:admin#delete igmp_snooping static_group vlan default 239.1.1.1
Command: delete igmp_snooping static_group vlan default 239.1.1.1

Success.

DES-3200-28P:admin#
```

30-11 config igmp_snooping static_group

Description

This command is used to configure IGMP snooping static group. When a port is configured as a static member port, the IGMP protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by IGMP. If this port is configured as a static member later, then the IGMP protocol will stop operating on this port. The IGMP protocol will resume once this port is removed from static member ports.

The static member port will only affect V2 IGMP operation.

Format

config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>

Parameters

vlan - Specify the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long. **vlanid** - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specify the multicast group IP address (for Layer 3 switch). **add** - Specify to add the member ports. **delete** - Specify to delete the member ports.
<portlist> - Specify a range of ports to be configured.

Restrictions

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

Example

To unset port range 9-10 from IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
DES-3200-28P:admin#config igmp_snooping static_group vlan default 239.1.1.1
delete 9-10
Command: create igmp_snooping static_group vlan default 239.1.1.1 delete 9-10

Success.

DES-3200-28P:admin#
```

30-12 show igmp_snooping static_group

Description

This command is used to display the IGMP snooping multicast group static members.

Format

show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}

Parameters

vlan - Specify the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long. **vlanid** - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specify the multicast group IP address.

Restrictions

None.

Example

To display all the IGMP snooping static groups:

```
DES-3200-28P:admin#show igmp_snooping static_group
VLAN ID/Name         IP Address            Static Member Ports
--------------   ------------------    ------------------------
1 / Default          239.1.1.1              9-10



Total Entries : 1
DES-3200-28P:admin#
```

30-13 config igmp_snooping data_driven_learning

Description

This command is used to enable or disable the data driven learning of an IGMP snooping group.

When data-driven learning is enabled for the VLAN, when the Switch receives the IP multicast traffic on this VLAN, an IGMP snooping group will be created. That is, the learning of an entry is not activated by IGMP membership registration, but activated by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.

When data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.

Note that if a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. That is, the aging out mechanism will follow the ordinary IGMP snooping entry.

Format

config igmp_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

Parameters

all - Specify all VLANs to be configured.
vlan_name - Specify the VLAN name to be configured. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specify the VLAN ID to be configured. **<vlanid_list>** - Enter the VLAN ID here.

state - (Optional) Specify to enable or disable the data driven learning of an IGMP snooping group. **enable** - Enter enable to enable the data driven learning option. By default, the state is enabled. **disable** - Enter disable to disable the data driven learning option.
aged_out - (Optional) Enable or disable the aging out of the entry. **enable** - Enter enable to enable the aging out of the entry. **disable** - Enter disable to disable the aging out of the entry. By default, the state is disabled state.
expiry_time - (Optional) Specify the data driven group lifetime in seconds. This parameter is valid only when aged_out is enabled. **<sec 1-65535>** - Enter the expiry time here. This value must be between 1 and 65535 seconds.

Restrictions

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

Example

To enable the data driven learning of an IGMP snooping group on the default VLAN:

```
DES-3200-28P:admin#config igmp_snooping data_driven_learning vlan_name default
state enable
Command: config igmp_snooping data_driven_learning vlan_name default state
enable

Success.

DES-3200-28P:admin#
```

30-14 config igmp_snooping data_driven_learning max_learned_entry

Description

This command is used to configure the maximum number of groups that can be learned by data driven.

When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the new groups will be dropped.

Format

config igmp_snooping data_driven_learning max_learned_entry <value 1-1024>

Parameters

max_learned_entry - Specify the maximum number of groups that can be learned by data driven. The default setting is 128. **<value 1-1024>** - Enter the maximum learning entry value here. This value must be between 1 and 1024.

Restrictions

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

Example

To set the maximum number of groups that can be learned by data driven:

```
DES-3200-28P:admin#config igmp_snooping data_driven_learning max_learned_entry
50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.

DES-3200-28P:admin#
```

30-15 clear igmp_snooping data_driven_group

Description

This command is used to delete the IGMP snooping group(s) learned by data driven.

Format

clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr> | all]]

Parameters

all - Specify all VLANs to which IGMP snooping groups will be deleted.
vlan_name - Specify the VLAN name. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specify the VLAN ID. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specify the group's IP address learned by data driven.
all - Delete all IGMP snooping groups of specified VLANs.

Restrictions

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

Example

To delete all the groups learned by data-driven:

```
DES-3200-28P:admin#clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.

DES-3200-28P:admin#
```

30-16 show igmp_snooping

Description

This command is used to display the current IGMP snooping configuration on the Switch.

Format

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specify the name of the VLAN for which you want to view the IGMP snooping configuration. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN for which you want to view the IGMP snooping configuration. **<vlanid_list>** - Enter the VLAN ID list here.
If the VLAN is not specified, the system will display all current IGMP snooping configurations.

Restrictions

None.

Example

To show IGMP snooping:

```
DES-3200-28P:admin#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State              : Enabled
 Data Driven Learning Max Entries        : 128

 VLAN Name                     : default
 Query Interval                : 125
 Max Response Time             : 10
 Robustness Value              : 2
 Last Member Query Interval    : 1
 Querier State                 : Disabled
 Querier Role                  : Non-Querier
 Querier IP                    : 0.0.0.0
 Querier Expiry Time           : 0 secs
 State                         : Disabled
 Fast Leave                    : Disabled
 Rate Limit                    : No Limitation
 Report Suppression            : Enabled
 Version                       : 3
 Data Driven Learning State    : Enabled
 Data Driven Learning Aged Out : Disabled
 Data Driven Group Expiry Time : 260

Total Entries: 1


DES-3200-28P:admin#
```

30-17 show igmp_snooping rate_limit

Description

This command is used to display the IGMP snooping rate limit setting.

Format

show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

Parameters

ports - Specify the port range. **<portlist>** - Enter the range of ports here.
vlanid - Specify the VLAN range.. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the IGMP snooping rate limit for ports 1 to 15:

```
DES-3200-28P:admin#show igmp_snooping rate_limit ports 1-15
Command: show igmp_snooping rate_limit ports 1-15

Port         Rate Limit
--------    -----------
 1            No Limit
 2            100
 3            No Limit
 4            No Limit
 5            No Limit

Total Entries: 5
```

30-18 show igmp_snooping group

Description

This command is used to display the current IGMP snooping group configuration on the Switch.

Format

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}

Parameters

vlan - (Optional) Specify the name of the VLAN for which you want to view IGMP snooping group information. If VLAN, ports and IP address are not specified, the system will display all current IGMP snooping group information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN for which you want to view IGMP snooping group information. **<vlanid_list>** - Enter the VLAN ID list here.
ports - (Optional) Specify a list of ports for which you want to view IGMP snooping group information. **<portlist>** - Enter the list of ports here.
<ipaddr> - (Optional) Specify the group IP address for which you want to view IGMP snooping group information.
data_driven - (Optional) If data_driven is specified, only data driven groups will be displayed.

Restrictions

None.

Example

To show IGMP snooping groups when IGMP v3 is supported:

```
DES-3200-28P:admin#show igmp_snooping group
Command: show igmp_snooping group

Source/Group                    : 10.0.0.1/225.0.0.1
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 6
 Expiry Time                    : 254
 Filter Mode                    : INCLUDE

 Source/Group                   : 10.0.0.10/225.0.0.1
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 6
 Expiry Time                    : 254
 Filter Mode                    : INCLUDE

 Source/Group                   : NULL/239.255.255.250
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 2
 Expiry Time                    : 258
 Filter Mode                    : EXCLUDE

 Total Entries: 3

DES-3200-28P:admin#
```

```
DES-3200-28P:admin#show igmp_snooping group data_driven
Command: show igmp_snooping group data_driven
Source/Group        : NULL/225.0.0.5
VLAN Name/VID       : default/1
Reports             : 0
Member Ports        :
Router Ports        : 24
UP Time             : 3 days 50 mins
Expiry Time         : 120 secs
Filter Mode         : EXCLUDE

Total Entries : 1

DES-3200-28P:admin#
```

To show IGMP snooping groups when only IGMP v2 is supported: The third item is a data-driven learned entry. If the member port list is empty, the multicast packets will be forwarded to the router ports. If the router port list is empty, the packets will be dropped.

```
DES-3200-28P:admin#show igmp_snooping group
Command: show igmp_snooping group

Source/Group                   : NULL/226.0.0.1
 VLAN Name/VID                  : default/1
```

```
 Member Ports                  : 5
 UP Time                       : 10
 Expiry Time                   : 258
 Filter Mode                   : EXCLUDE

 Source/Group                  : NULL/226.0.0.2
 VLAN Name/VID                 : default/1
 Member Ports                  : 5
 UP Time                       : 9
 Expiry Time                   : 259
 Filter Mode                   : EXCLUDE

 Source/Group                  : NULL/226.0.0.3
 VLAN Name/VID                 : default/1
 Member Ports                  :
 Router Ports                  :
 UP Time                       : 1
 Expiry Time                   : 259
 Filter Mode                   : EXCLUDE

 Source/Group                  : NULL/239.255.255.250
 VLAN Name/VID                 : default/1
 Member Ports                  : 5
 UP Time                       : 1
 Expiry Time                   : 259
 Filter Mode                   : EXCLUDE

 Total Entries: 4

DES-3200-28P:admin#
```

30-19 show igmp_snooping forwarding

Description

This command is used to display the Switch's current IGMP snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from a specific sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The IGMP snooping further restricts the forwarding ports.

Format

show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specify the name of the VLAN for which you want to view IGMP snooping forwarding table information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN for which you want to view IGMP snooping forwarding table information.

<vlanid_list> - Enter the VLAN ID list here.
If no parameter is specified, the system will display all current IGMP snooping forwarding table entries of the Switch.

Restrictions

None.

Example

To show all IGMP snooping forwarding entries located on the Switch:

```
DES-3200-28P:admin#show igmp_snooping forwarding
Command: show igmp_snooping forwarding

VLAN Name      : default
Source IP      : *
Multicast Group: 225.0.0.0
Port Member    : 2,7

VLAN Name      : default
Source IP      : *
Multicast Group: 225.0.0.1
Port Member    : 2,5

VLAN Name      : default
Source IP      : *
Multicast Group: 225.0.0.2
Port Member    : 2,8

Total Entries : 3

DES-3200-28P:admin#
```

30-20 show router_ports

Description

This command is used to display the currently configured router ports on the Switch.

Format

show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

Parameters

vlan - Specify the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.

all - Specify all VLANs on which the router port resides.
static - (Optional) Displays router ports that have been statically configured.
dynamic - (Optional) Displays router ports that have been dynamically configured.
forbidden - (Optional) Displays forbidden router ports that have been statically configured.
If no parameter is specified, the system will display all currently configured router ports on the Switch.

Restrictions

None.

Example

To display router ports:

```
DES-3200-28P:admin#show router_ports all
Command: show router_ports all

VLAN Name               : default
Static Router Port      : 1-10
Dynamic Router Port     :
          Router IP     : 10.0.0.1, 10.0.0.2, 10.0.0.3
Forbidden router port   :

VLAN Name               : vlan2
Static router port      :
Dynamic router port     : 13
          Router IP     : 10.0.0.4, 10.0.0.5, 10.0.0.6
Forbidden router port   :

Total Entries : 2

DES-3200-28P:admin#
```

30-21 show igmp_snooping statistics counter

Description

This command is used to display the statistics counter for IGMP protocol packets that are received by the Switch since IGMP snooping was enabled.

Format

show igmp_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]

Parameters

vlan - Specify a VLAN to be displayed. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specify a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specify a list of ports to be displayed.

<portlist> - Enter the list of port to be displayed here.

Restrictions

None.

Example

To display the IGMP snooping statistics counter:

```
DES-3200-28P:admin#show igmp_snooping statistic counter vlanid 67
Command: show igmp_snooping statistic counter vlanid 67

VLAN Name         : VLAN67
-------------------------------------------------
Group Number      : 0

Receive Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 0
      Dropped By Multicast VLAN        : 0

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 0
      Dropped By Max Group Limitation  : 0
      Dropped By Group Filter          : 0
      Dropped By Multicast VLAN        : 0

Transmit Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 44
      IGMP v3 Query                    : 0
      Total                            : 44

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0

 Total Entries : 1
```

```
DES-3200-28P:admin#
```

To display the IGMP snooping statistics counter for a port:

```
DES-3200-28P:admin#show igmp_snooping statistic counter ports 1
Command: show igmp_snooping statistic counter ports 1

Port #            : 1
--------------------------------------------------
Group Number      : 0

Receive Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 0
      Dropped By Multicast VLAN        : 0

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 0
      Dropped By Max Group Limitation  : 0
      Dropped By Group Filter          : 0
      Dropped By Multicast VLAN        : 0

Transmit Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 0
      Total                            : 0

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0

 Total Entries : 1

DES-3200-28P:admin#
```

30-22 show igmp access_authentication ports

Description

This command is used to display the current IGMP Access Control configuration.

Format

show igmp access_authentication ports [all | <portlist>]

Parameters

all - Specify all ports to be displayed.
<portlist> - Specify a range of ports to be displayed.

Restrictions

None.

Example

To display the IGMP Access Control status for ports 1-4:

```
DES-3200-28P:admin#show igmp access_authentication ports 1-4
Command: show igmp access_authentication ports 1-4

Port     State
-----    ---------
1        Enabled
2        Disabled
3        Disabled
4        Disabled

DES-3200-28P:admin#
```

To display the IGMP Access Control status for all ports:

```
DES-3200-28P:admin#show igmp access_authentication ports all
Command: show igmp access_authentication ports all

Port     State
-----    ---------
1        Enabled
2        Disabled
3        Disabled
4        Disabled
5        Disabled
6        Disabled
7        Disabled
8        Disabled
9        Disabled
10       Disabled
11       Disabled
```

```
12       Disabled
13       Disabled
14       Disabled
15       Disabled
16       Disabled
17       Disabled
18       Disabled
19       Disabled
20       Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

30-23 clear igmp_snooping statistics counter

Description

This command is used to clear the IGMP snooping statistics counter.

Format

clear igmp_snooping statistics counter

Parameters

None.

Restrictions

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

Example

To clear the IGMP snooping statistics counter:

```
DES-3200-28P:admin#clear igmp_snooping statistic counter
Command: clear igmp_snooping statistic counter

Success.

DES-3200-28P:admin#
```

30-24 config mld_snooping

Description

This command is used to configure MLD snooping on the Switch.

Format

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | report_suppression [enable | disable]

Parameters

vlan_name - Specify the name of the VLAN for which MLD snooping is to be configured. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN for which MLD snooping is to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specify all VLANs for which MLD snooping is to be configured.
state - Enable or disable MLD snooping for the chosen VLAN. **enable** - Enter enable here to enable MLD snooping for the chosen VLAN. **disable** - Enter disable here to disable MLD snooping for the chosen VLAN.
fast_done - Enable or disable MLD snooping fast done function. **enable** - Enable the MLD snooping fast done function. If enable, the membership is immediately removed when the system receive the MLD leave message. **disable** - Disable the MLD snooping fast done function.
report_suppression - Specify MLD snooping report suppression. **enable** - Enable the MLD snooping report suppression function. **disable** - Disable the MLD snooping report suppression function.

Restrictions

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

Example

To configure MLD snooping:

```
DES-3200-28P:admin#config mld_snooping vlan_name default state enable
Command: config mld_snooping vlan_name default state enable

Success.

DES-3200-28P:admin#
```

30-25 config mld_snooping querier

Description

This command is used to configure the timer in seconds between general query transmissions, the maximum time in seconds to wait for reports from listeners, and the permitted packet loss that is guaranteed by MLD snooping.

Format

config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}

Parameters

vlan_name - Specify the name of the VLAN for which MLD snooping querier is to be configured. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN for which MLD snooping querier is to be configured.

<vlanid_list> - Enter the VLAN ID list here. **all** - Specify all VLANs for which MLD snooping querier is to be configured.
query_interval - Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds. **<sec 1-65535>** - Enter the query interval value here. This value must be between 1 and 65535 seconds.
max_reponse_time - Specify the maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds. **<sec 1-25>** - Enter the maximum response time value here. This value must be between 1 and 25 seconds.
robustness_variable - Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals: **<value 1-7>** - Enter the robustness variable value here. This value must be between 1 and 7. • Group listener interval—Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval). • Last listener query count—Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely.
last_listener_query_interval - (Optional) Specify the maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group. The default setting is 1 second. **<sec 1-25>** - Enter the last listener query interval value here. This value must be between 1 and 25 seconds.
state - (Optional) This allows the Switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable. **enable** - Enable the MLD querier state. **disable** - Disable the MLD querier state.
version - (Optional) Specify the version of MLD packet that will be sent by the Switch. **<value 1-2>** - Enter the version number value here. This value must be between 1 and 2.

Restrictions

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

Example

To configure the MLD snooping querier:

```
DES-3200-28P:admin#config mld_snooping querier vlan_name default query_interval
125 state enable
Command: config mld_snooping querier vlan_name default query_interval 125 state
enable

Success.

DES-3200-28P:admin#
```

30-26 config mld_snooping router_ports

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol, etc.

Format

config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

vlan - Specify the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specify to add the router ports.
delete - Specify to delete the router ports.
<portlist> - Specify a range of ports to be configured.

Restrictions

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

Example

To set up static router ports:

```
DES-3200-28P:admin#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

DES-3200-28P:admin#
```

30-27 config mld_snooping router_ports_forbidden

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Format

config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

vlan - Specify the name of the VLAN on which the forbidden router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN on which the forbidden router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specify to add the forbidden router ports.
delete - Specify to delete the forbidden router ports.
<portlist> - Specify a range of ports to be configured.

Restrictions

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

Example

To set up port 11 as the forbidden router port of the default VLAN:

```
DES-3200-28P:admin#config mld_snooping mrouter_ports_forbidden vlan default add
11
Command: config mld_snooping mrouter_ports_forbidden vlan default add 11

Success.

DES-3200-28P:admin#
```

30-28 enable mld_snooping

Description

This command is used to enable MLD snooping on the Switch. MLD snooping is disabled by default.

Format

enable mld_snooping

Parameters

When the Switch receives an MLD report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.

Restrictions

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

Example

To enable MLD snooping on the Switch:

```
DES-3200-28P:admin#enable mld_snooping
Command: enable mld_snooping

Success.

DES-3200-28P:admin#
```

30-29 disable mld_snooping

Description

This command is used to disable MLD snooping on the Switch.

Format

disable mld_snooping

Parameters

When the Switch receives an MLD report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.

Restrictions

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

Example

To disable MLD snooping on the Switch:

```
DES-3200-28P:admin#disable mld_snooping
Command: disable mld_snooping

Success.

DES-3200-28P:admin#
```

30-30 show mld_snooping

Description

This command is used to display the current MLD snooping configuration on the Switch.

Format

show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specify the name of the VLAN for which you want to view the MLD snooping

configuration. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN for which you want to view the MLD snooping configuration. **<vlanid_list>** - Enter the VLAN ID list here.
If VLAN is not specified, the system will display all current MLD snooping configurations.

Restrictions

None.

Example

To show MLD snooping:

```
DES-3200-28P:admin#show mld_snooping
Command: show mld_snooping

 MLD Snooping Global State               : Enabled
 Data Driven Learning Max Entries        : 128

 VLAN Name                     : default
 Query Interval                : 125
 Max Response Time             : 10
 Robustness Value              : 2
 Last Listener Query Interval  : 1
 Querier State                 : Enabled
 Querier Role                  : Querier
 Querier IP                    : FE80::201:2FF:FE03:400
 Querier Expiry Time           : 0 secs
 State                         : Enabled
 Fast Done                     : Disabled
 Rate Limit                    : No Limitation
 Report Suppression            : Enabled
 Version                       : 2
 Data Driven Learning State    : Enabled
 Data Driven Learning Aged Out : Disabled
 Data Driven Group Expiry Time : 260

Total Entries: 1


DES-3200-28P:admin#
```

30-31 show mld_snooping group

Description

This command is used to display the current MLD snooping group information on the Switch.

Format

show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}} {data_driven}

Parameters

vlan - (Optional) Specify the name of the VLAN for which you want to view MLD snooping group information. If VLAN and ports and IP address are not specified, the system will display all current MLD snooping group information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN for which you want to view MLD snooping group information. **<vlanid_list>** - Enter the VLAN ID list here.
ports - (Optional) Specify a list of ports for which you want to view MLD snooping group information. **<portlist>** - Enter the list of port here.
<ipv6addr> - (Optional) Specify the group IPv6 address for which you want to view MLD snooping group information.
data_driven - (Optional) Display the data driven groups.

Restrictions

None.

Example

To show an MLD snooping group when MLD v2 is supported:

The first two items mean that for ports 1-2 / port 3, the data from the FE1E::1 will be forwarded.

The third item means that for ports 4-5, the data from FE1E::2 will be forwarded.

The fourth item is a data-driven learned entry. The member port list is empty. The multicast packets will be forwarded to the router ports. If the router port list is empty, the packet will be dropped.

```
DES-3200-28P:admin#show mld_snooping group
Command: show mld_snooping group

Source/Group        : 2001::1/FE1E::1
VLAN Name/VID       : default/1
Member Ports        : 1-2
UP Time             : 26
Expiry Time         : 258
Filter Mode         : INCLUDE

Source/Group        : 2002::2/FE1E::1
VLAN Name/VID:      : default/1
Member Ports        : 3
UP Time             : 29
Expiry Time         : 247
Filter Mode         : EXCLUDE

Source/Group        : NULL/FE1E::2
VLAN Name/VID       : default/1
Member Ports        : 4-5
UP Time             : 40
Expiry Time         : 205
Filter Mode         : EXCLUDE

Source/Group        : NULL/FF1E::5
VLAN Name/VID       : default/1
Member Ports        :
Router Ports        : 24
UP Time             : 100
Expiry Time         : 200
Filter Mode         : EXCLUDE

Total Entries : 4

DES-3200-28P:admin#
```

```
DES-3200-28P:admin#show mld_snooping group data_driven
Command: show mld_snooping group data_driven

Source/Group        : NULL/FF1E::5
VLAN Name/VID       : default/1
Member Ports        :
Router Ports        : 24
UP Time             : 100
Expiry Time         : 200
Filter Mode         : EXCLUDE

Total Entries : 1

DES-3200-28P:admin#
```

30-32 show mld_snooping forwarding

Description

This command is used to display the Switch's current MLD snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from specific sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN.

Format

show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specify the name of the VLAN for which you want to view MLD snooping forwarding table information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN for which you want to view MLD snooping forwarding table information. **<vlanid_list>** - Enter the VLAN ID list here.
If no parameter is specified, the system will display all current MLD snooping forwarding table entries of the Switch.

Restrictions

None.

Example

To show all MLD snooping forwarding entries located on the Switch.

```
DES-3200-28P:admin#show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name      : default
Source IP      : *
Multicast Group: FE1E::1
Port Member    : 2,7

VLAN Name      : default
Source IP      : *
Multicast Group: FF1E::1
Port Member    : 5

Total Entries : 2

DES-3200-28P:admin#
```

30-33 show mld_snooping mrouter_ports

Description

This command is used to display the currently configured router ports on the Switch.

Format

show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

Parameters

vlan - Specify the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specify all VLANs on which the router port resides.
static - (Optional) Displays router ports that have been statically configured.
dynamic - (Optional) Displays router ports that have been dynamically configured.
forbidden - (Optional) Displays forbidden router ports that have been statically configured.
If no parameter is specified, the system will display all currently configured router ports on the Switch.

Restrictions

None.

Example

To display the mld_snooping mrouter ports:

```
DES-3200-28P:admin#show mld_snooping mrouter_ports vlan default
Command: show mld_snooping mrouter_ports vlan default


VLAN Name                : default
Static Router Port       : 1-10
Dynamic Router Port      :
Router IP                :
Forbidden Router Port    : 11

 Total Entries: 1


DES-3200-28P:admin#
```

30-34 create mld_snooping static_group

Description

This command is used to create an MLD snooping static group. Member ports can be added to the static group. The static member and the dynamic member ports form the member ports of a group.

The static group will only take effect when MLD snooping is enabled on the VLAN. An **active** static group must be equal to a static MLD group with a link-up member port. For those static member ports, the device needs to emulate the MLD protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

The Reserved IP multicast addresses FF0x::/16 must be excluded from the configured group.

The VLAN must be created first before a static group can be created.

Format

create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Parameters

vlan - Specify the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Specify the multicast group IPv6 address.

Restrictions

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

Example

To create an MLD snooping static group for VLAN 1, group FF1E::1:

```
DES-3200-28P:admin#create mld_snooping static_group vlan default FF1E::1
Command: create mld_snooping static_group vlan default FF1E::1

Success.

DES-3200-28P:admin#
```

30-35 delete mld_snooping static_group

Description

This command is used to delete a MLD Snooping multicast static group.

Format

delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Parameters

vlan - Specify the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN on which the static group resides.

<vlanid_list> - Enter the VLAN ID list here.
<ipv6addr> - Specify the multicast group IP address.

Restrictions

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

Example

To delete an MLD snooping static group for VLAN 1, group FF1E::1:

```
DES-3200-28P:admin#delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

DES-3200-28P:admin#
```

30-36 config mld_snooping static_group

Description

This command is used to configure an MLD snooping multicast group static member port. When a port is configured as a static member port, the MLD protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by MLD. If this port is configured as a static member later, then the MLD protocol will stop operating on this port. The MLD protocol will resume once this port is removed from static member ports.

Format

config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>

Parameters

vlan - Specify the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Specify the multicast group IPv6 address.
add - Specify to add the member ports. **delete** - Specify to delete the member ports.
<portlist> - Specify a range of ports to be configured.

Restrictions

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

Example

To unset port range 9-10 from MLD snooping static member ports for group FF1E::1 on default VLAN:

```
DES-3200-28P:admin#config mld_snooping static_group vlan default FF1E::1 delete
9-10
Command: config mld_snooping static_group vlan default FF1E::1 delete 9-10

Success.

DES-3200-28P:admin#
```

30-37 show mld_snooping static_group

Description

This command used to display the MLD snooping multicast group static members.

Format

show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}

Parameters

vlan - (Optional) Specify the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - (Optional) Specify the multicast group IPv6 address.

Restrictions

None.

Example

To display all the MLD snooping static groups:

```
DES-3200-28P:admin#show mld_snooping static_group
VLAN ID/Name         IP Address            Static Member Ports
--------------   ------------------    ------------------------
1 / Default          FF1E ::1              9-10

Total Entries : 1

DES-3200-28P:admin#
```

30-38 config mld_snooping data_driven_learning

Description

This command is used to enable or disable the data-driven learning of an MLD snooping group.

When data-driven learning is enabled for the VLAN, when the Switch receives the IP multicast traffic, on this VLAN, an MLD snooping group will be created. That is, the learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD

snooping entry, the MLD protocol will take care the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.

When the data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.

Note that if a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. That is, the aging out mechanism will follow the ordinary MLD snooping entry.

Format

config mld_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

Parameters

all - Specify that all VLANs are to be configured.
vlan_name - Specify the VLAN name to be configured. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specify the VLAN ID to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
state - (Optional) Specify to enable or disable the data driven learning of MLD snooping groups. By default, the state is enabled. **enable** - Enter enable to enable the data driven learning state. **disable** - Enter disable to disable the data driven learning state.
aged_out - (Optional) Enable or disable the aging out of entries. By default, the state is disabled. **enable** - Enter enable to enable the aged out option. **disable** - Enter disable to disable the aged out option.
expiry_time - (Optional) Specify the data driven group lifetime, in seconds. This parameter is valid only when aged_out is enabled. **<sec 1-65535>** - Enter the expiry time value here. This value must be between 1 and 65535 seconds.

Restrictions

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

Example

To enable the data driven learning of an MLD snooping group on the default VLAN:

```
DES-3200-28P:admin#config mld_snooping data_driven_learning vlan default state
enable
Command: config mld_snooping data_driven_learning vlan default state enable

Success.

DES-3200-28P:admin#
```

30-39 config mld_snooping data_driven_learning max_learned_entry

Description

This command is used to configure the maximum number of groups that can be learned by data driven.

When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the new groups will be dropped.

Format

config mld_snooping data_driven_learning max_learned_entry <value 1-1024>

Parameters

max_learned_entry - Specify the maximum number of groups that can be learned by data driven. The default setting is 128.
<value 1-1024> - Enter the maximum learned entry value here. This value must be between 1 and 1024.

Restrictions

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

Example

To set the maximum number of groups that can be learned by data driven:

```
DES-3200-28P:admin#config mld_snooping data_driven_learning max_learned_entry
50
Command: config mld_snooping data_driven_learning max_learned_entry 50

Success.

DES-3200-28P:admin#
```

30-40 clear mld_snooping data_driven_group

Description

This command is used to delete the MLD snooping groups learned by data driven.

Format

clear mld_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipv6addr>| all]]

Parameters

all - Specify all VLANs to which MLD snooping groups will be deleted.
vlan_name - Specify the VLAN name.

<vlan_name> - Enter the VLAN name here.
vlanid - Specify the VLAN ID. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Specify the group's IP address learned by data driven.
all - Specify to clear all data driven groups of the specified VLAN.

Restrictions

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

Example

To clear all the groups learned by data-driven:

```
DES-3200-28P:admin#clear mld_snooping data_driven_group all
Command: clear mld_snooping data_driven_group all

Success.

DES-3200-28P:admin#
```

30-41 show mld_snooping statistic counter

Description

This command is used to display the statistics counter for MLD protocol packets that are received by the Switch since MLD snooping was enabled.

Format

show mld_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]

Parameters

vlan - Specify a VLAN to be displayed. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specify a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specify a list of ports to be displayed. **<portlist>** - Enter the list of port here.

Restrictions

None.

Example

To show MLD snooping statistics counters:

```
DES-3200-28P:admin# show mld_snooping statistic counter vlanid 1
Command: show mld_snooping statistic counter vlanid 1

VLAN Name  : Default
-----------------------------------------------
  Total Groups          : 10
Receive Statistics
      Query
MLD v1 Query                    : 1
MLD v2 Query                    : 1
Total                           : 2
Dropped By Rate Limitation      : 1
Dropped By Multicast VLAN       : 1

  Report & Leave
MLD v1 Report                   : 0
MLD v2 Report                   : 10
MLD v1 Done                     : 1
Total                           : 11
Dropped By Rate Limitation      : 0
Dropped By Max Group Limitation : 90
Dropped By Group Filter         : 0
Dropped By Multicast VLAN       : 1

Transmit Statistics
Query
MLD v1 Query                    : 1
MLD v2 Query                    : 1
Total                           : 2
Report & Leave
MLD v1 Report                   : 0
MLD v2 Report                   : 10
MLD v1 Done                     : 1
Total                           : 11

Total Entries : 1

DES-3200-28P:admin#
```

30-42 clear mld_snooping statistics counter

Description

This command is used to clear MLD snooping statistics counters.

Format

clear mld _snooping statistics counter

Parameters

None.

Restrictions

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

Example

To clear MLD snooping statistics counter:

```
DES-3200-28P:admin#clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter

Success.

DES-3200-28P:admin#
```

30-43 config mld_snooping rate_limit

Description

This command is used to configure the rate limit of MLD control packets that are allowed by each port or VLAN.

Format

config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Parameters

ports - Specify a range of ports to be configured. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specify a range of VLANs to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
<value 1-1000> - Configure the rate limit of MLD control packets that the Switch can process on a specific port or VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped.
no_limit - Configure the rate limit of MLD control packets that the Switch can process on a specific port or VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped. The default setting is no_limit.

Restrictions

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

Example

To configure the MLD snooping per port rate limit:

```
DES-3200-28P:admin#config mld_snooping rate_limit ports 1 100
Command: config mld_snooping rate_limit ports 1 100

Success.

DES-3200-28P:admin#
```

30-44 show mld_snooping rate_limit

Description

This command is used to display the rate limit of MLD control packets that are allowed by each port or VLAN.

Format

show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

Parameters

ports - Specify a list of ports. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specify a list of VLANs. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the MLD snooping rate limit from port 1 to 5:

```
DES-3200-28P:admin#show mld_snooping rate_limit ports 1-5
Command: show mld_snooping rate_limit ports 1-5

 Port      Rate Limit
 --------  ---------------
 1         100
 2         No Limit
 3         No Limit
 4         No Limit
 5         No Limit

Total Entries: 5

DES-3200-28P:admin#
```

Chapter 31 IP-MAC-Port Binding (IMPB) Command List

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}
delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]
delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]
config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
show address_binding {ports {<portlist>}}
show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]
show address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]
show address_binding {[ip_mac [all | [[ipaddress <ipaddr>] [mac_address <macaddr>]] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>] | ports {<portlist>}]}
enable address_binding dhcp_snoop
disable address_binding dhcp_snoop
clear address_binding dhcp_snoop binding_entry ports [<portlist> | all]
show address_binding dhcp_snoop {max_entry {ports <portlist>}}
show address_binding dhcp_snoop binding_entry {port <port>}
config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit]
enable address_binding trap_log
disable address_binding trap_log
config address_binding recover_learning ports [<portlist> | all]
debug address_binding [event | dhcp | all] state [enable | disable]
no debug address_binding

31-1 create address_binding ip_mac

Description

This command is used to create an IMPB entry.

Format

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

ipaddress - Specify the IP address used for the IMPB entry. **<ipaddr>** - Enter the IP address used here.
mac_address - Specify the MAC address used for the IMPB entry. **<macaddr>** - Enter the MAC address used here.
ports - (Optional) Specify the portlist the entry will apply to. If not ports are specified, the settings will be applied to all ports. **<portlist>** - Enter a list of ports used for this configuration here. **all** - Specify that all the ports will be included.

Restrictions

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

Example

To create an IMPB entry:

```
DES-3200-28P:admin#create address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11

Success.

DES-3200-28P:admin#
```

31-2 config address_binding ip_mac ports

Description

This command is used to configure the state of IMPB on the Switch for each port.

Format

config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}

Parameters

ports - Specify the ports used for this configuration. **<portlist>** - Enter the list of ports used for this configuration here. **all** - Specify that all the ports will be used.
arp_inspection - (Optional) Specify that the ARP inspection option will be configured. **strict** - In this mode, all packets are dropped by default until a legal ARP or IP packets are detected. **loose** - In this mode, all packets are forwarded by default until an illegal ARP or broadcast IP packets are detected. If not specified strict or loose, default is strict. **disable** - Disable ARP inspection function. The default value is disabled.
ip_inspection - (Optional) Specify that the IP inspection option will be configured. **enable** - Enable IP inspection function. The legal IP packets will be forwarded, while the illegal IP packets will be dropped. **disable** - Disable IP inspection function. The default value is disabled.
protocol - (Optional) Specify the version used. **ipv4** - Only IPv4 packets will be checked.
allow_zeroip - (Optional) Specify whether to allow ARP packets with a source IP address of 0.0.0.0. If the IP address 0.0.0.0 is not configured in the binding list and this setting is enabled, ARP packets with the source IP address of 0.0.0.0 will be allowed; If the IP address 0.0.0.0 is not configured in the binding list and this setting is disabled, ARP packets with the source IP address of 0.0.0.0 will not be allowed. This option does not affect the IMPB ACL Mode. **enable** - Specify that the allow zero IP option will be enabled. **disable** - Specify that the allow zero IP option will be disabled.
forward_dhcppkt - (Optional) By default, DHCP packets with a broadcast DA will be flooded.

When set to disabled, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP Snooping is enabled, in this case DHCP packets trapped by the CPU must be forwarded by the software. This setting controls the forwarding behavior in this situation.
enable - Specify that the forward DHCP packets option will be enabled.
disable - Specify that the forward DHCP packets option will be disabled.

stop_learning_threshold - (Optional) When the number of blocked entries exceeds the threshold, the port will stop learning new addresses. Packets with a new address will be dropped.
<int 0-500> - Enter the stop learning threshold value here. This value must be between 0 and 500.

Restrictions

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

Example

To enable IMPB on port 1:

```
DES-3200-28P:admin#config address_binding ip_mac ports 1 arp_inspection strict
Command: config address_binding ip_mac ports 1 arp_inspection strict

Success.

DES-3200-28P:admin#
```

31-3 delete address_binding blocked

Description

This command is used to delete a blocked entry.

Format

delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

Parameters

all - Specify that all the entries the address database that the system has automatically blocked to be deleted.

vlan_name - Specify the name of the VLAN to which the blocked MAC address belongs.
<vlan_name> - Enter the VLAN name.
mac_address - Specify the MAC address of the entry or the blocked MAC address.
<macaddr> - Enter the MAC address used.

Restrictions

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

Example

To delete a blocked address:

```
DES-3200-28P:admin#delete address_binding blocked vlan_name v31 mac_address 00-
00-00-00-00-11
Command: delete address_binding blocked vlan_name v31 mac_address 00-00-00-00-
00-11

Success.

DES-3200-28P:admin#
```

31-4 delete address_binding ip_mac

Description

This command is used to delete an IMPB entry.

Format

delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]

Parameters

all - Specify that all the MAC address will be used.
ipaddress - Specify the learned IP address of the entry in the database. **<ipaddr>** - Enter the IP address used. **mac_address** - Specify the MAC address used for this configuration. **<macaddr>** - Enter the MAC address used.

Restrictions

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

Example

To delete a blocked address:

```
DES-3200-28P:admin#delete address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11
Command: delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11

Success.

DES-3200-28P:admin#
```

31-5 config address_binding ip_mac ipaddress

Description

This command is used to update an IMPB entry.

Format

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

ipaddress - Specify the IP address of the entry being updated. **<ipaddr>** - Enter the IP address used here.
mac_address - Specify the MAC address of the entry being updated **<macaddr>** - Enter the MAC address used here.
ports - (Optional) Specify which ports are used for the IMPB entry being updated. If not specified, then it is applied to all ports. **<portlist>** - Enter the list of port used here. **all** - Specify that all the ports will be used.

Restrictions

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

Example

To configure an IMPB entry:

```
DES-3200-28P:admin#config address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11

Success.

DES-3200-28P:admin#
```

31-6 show address_binding

Description

This command is used to display the IMPB global settings or IMPB settings on specified ports.

Format

show address_binding {ports {<portlist>}}

Parameters

ports - (Optional) Specify the ports for which the information is displayed. If not specified, all ports are displayed. **<portlist>** - (Optional) Enter the list of ports used here.

Restrictions

None.

Example

To show the IMPB global configuration:

```
DES-3200-28P:admin#show address_binding
Command: show address_binding

Trap/Log          : Disabled
DHCP Snoop        : Disabled


DES-3200-28P:admin#
```

To show the IMPB ports:

```
DES-3200-28P:admin#show address_binding ports
Command: show address_binding ports


 ARP: ARP Inspection   IP: IP Inspection

 Port   ARP      IP     Protocol Zero IP   DHCP Packet  Stop Learning
                                                       Threshold/Mode
 ----- -------- --------  ----- ---------  -----------  --------------
 1     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 2     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 3     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 4     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 5     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 6     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 7     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 8     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 9     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 10    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 11    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 12    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 13    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 14    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 15    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 16    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

31-7 show address_binding blocked

Description

This command is used to display the blocked MAC entries.

Format

show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

Parameters

all - Specify that all the addresses in the database that the system has auto learned and blocked to be displayed.

vlan_name - Specify the name of the VLAN to which the blocked MAC address belongs. **<vlan_name>** - Enter the VLAN name used. **mac_address** - Specify the MAC address of the entry or the blocked MAC address. **<macaddr>** - Enter the MAC address of the entry or the blocked MAC address.

Restrictions

None.

Example

To show the IMPB entries that are blocked:

```
DES-3200-28P:admin#show address_binding blocked all
Command: show address_binding blocked all

 VID  VLAN Name                        MAC Address       Port
 ---- ------------------------------- ----------------- ----
 1    default                         00-0C-6E-AA-B9-C0 1

Total Entries : 1


DES-3200-28P:admin#
```

31-8 show address_binding ip_mac

Description

This command is used to display the IMPB entries.

Format

show address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]

Parameters

all - Specify that all the IP addresses to be displayed.
ipaddress - Specify the learned IP address of the entry in the database. **<ipaddr>** - Enter the learned IP address. **mac_address** - (Optional) Specify the MAC address of the entry in the database. **<macaddr>** - Enter the MAC address here.

Restrictions

None.

Example

To show IMPB entries:

```
DES-3200-28P:admin#show address_binding ip_mac all
Command: show address_binding ip_mac all

 M(Mode) - D:DHCP, S:Static ACL - A:Active I:Inactive

 IP Address                              MAC Address       M  ACL Ports
 --------------------------------------- ----------------- -- -- --------------
-
 10.1.1.1                                00-00-00-00-00-11 S  I  1-28

Total Entries : 1

DES-3200-28P:admin#
```

31-9 enable address_binding dhcp_snoop

Description

This command is used to enable DHCP snooping mode.

By default, DHCP snooping is disabled.

If a user enables DHCP Snooping mode, all ports which have IMPB disabled will become server ports. The switch will learn the IP addresses through server ports (by using DHCP Offer and DHCP ACK packets).

Note that the DHCP discover packet cannot be passed thru the user ports if the allow_zeroip function is disabled on the port.

The auto-learned IMPB entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an IP-Inspection mode binding entry for this specific port. Each entry is associated with a lease time. When the lease time has expires, the expired entry will be removed from the port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address has moved to a different port.

If a situation occurs where a binding entry learned by DHCP snooping conflicts with a statically configured entry. The binding relation has conflicted. For example, if IP A is binded to MAC X with a static configuration and suppose that the binding entry learned by DHCP snooping is that IP A is bound to MAC Y, and then it is conflict. When the DHCP snooping learned entry binds with the static configured entry, and the DHCP snooping learned entry will not be created.

In a situation where the same IMPB pair has been statically configured, the auto-learned entry will not be created. In a situation where the learned information is consistent with the statically configured entry the auto-learned entry will not be created. In a situation where the entry is statically configured in ARP mode the auto learned entry will not be created. In a situation where the entry is statically configured on one port and the entry is auto-learned on another port, the auto-learned entry will not be created.

Format

enable address_binding dhcp_snoop

Parameters

None.

Restrictions

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

Example

To enable DHCP IPv4 snooping mode:

```
DES-3200-28P:admin#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DES-3200-28P:admin#
```

31-10 disable address_binding dhcp_snoop

Description

This command is used to disable DHCP snooping mode. When the DHCP snooping function is disabled, all of the auto-learned binding entries will be removed.

Format

disable address_binding dhcp_snoop

Parameters

None.

Restrictions

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

Example

To disable DHCP IPv4 snooping mode:

```
DES-3200-28P:admin#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DES-3200-28P:admin#
```

31-11 clear address_binding dhcp_snoop binding_entry ports

Description

This command is used to clear the DHCP snooping entries learned for the specified ports.

Format

clear address_binding dhcp_snoop binding_entry ports [<portlist> | all]

Parameters

<portlist> - Enter the list of ports used.
all - Specify that all the ports will be used.

Restrictions

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

Example

To clear DHCP IPv4 snooping entries on ports 1-3:

```
DES-3200-28P:admin#clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DES-3200-28P:admin#
```

31-12 show address_binding dhcp_snoop

Description

This command is used to display the DHCP snooping configuration and learning database.

Format

show address_binding dhcp_snoop {max_entry {ports <portlist>}}

Parameters

max_entry - (Optional) To show the maximum number of entries per port.
ports - Specify the ports used for this configuration.
<portlist> - Enter a list of ports used here.
If no parameters are specified, show DHCP snooping displays the enable/disable state.

Restrictions

None.

Example

To show the DHCP snooping state:

```
DES-3200-28P:admin#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP_Snoop       : Disabled

DES-3200-28P:admin#
```

To display DHCP snooping maximun entry configuration:

```
DES-3200-28P:admin#show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry

Port  Max Entry
----  ---------
1     No Limit
2     No Limit
3     No Limit
4     No Limit
5     No Limit
6     No Limit
7     No Limit
8     No Limit
9     No Limit
10    No Limit
11    No Limit
12    No Limit
13    No Limit
14    No Limit
15    No Limit
16    No Limit
17    No Limit
18    No Limit
19    No Limit
20    No Limit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

31-13 show address_binding dhcp_snoop binding_entry

Description

This command is used to display the DHCP snooping binding entries.

Format

show address_binding dhcp_snoop binding_entry {port <port>}

Parameters

port – (Optional) Specify the port used for this configuration.

<port> - Enter the port number used here.

Restrictions

None.

Example

To display the DHCP snooping binding entries:

```
DES-3200-28P:admin#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

S (Status) - A: Active, I: Inactive
Time - Left Time (sec)

IP Address                              MAC Address           S  Time  Port
--------------------------------------- --------------------- -- ----- ------
10.62.58.35                             00-0B-5D-05-34-0B     A  35964  1
10.33.53.82                             00-20-c3-56-b2-ef     I  2590   2

Total entries : 2

DES-3200-28P:admin#
```

31-14 config address_binding dhcp_snoop max_entry

Description

This command is used to specify the maximum number of entries that can be learned by a specified port.

Format

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit]

Parameters

ports - Specify the list of ports you would like to set the maximum number of entries that can be learned.
<portlist> - Enter the list of ports used here.
all - Specify that all the ports will be used.

limit - Specify the maximum number. The default value is no_limit.
<value 1-50> - Enter the limit value here. This value must be between 1 and 50.
no_limit - Specify that the maximum number of learned entries is unlimited.

Restrictions

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

Example

To set the maximum number of DHCP IPv4 snooping entries that ports 1–3 can learned to 10:

```
DES-3200-28P:admin#config address_binding dhcp_snoop max_entry ports 1-3 limit
10.
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10.

Success.

DES-3200-28P:admin#
```

31-15 enable address_binding trap_log

Description

This command is used to send traps and logs when the IMPB module detects an illegal IP and MAC address.

Format

enable address_binding trap_log

Parameters

None.

Restrictions

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

Example

To enable the IMPB traps and logs:

```
DES-3200-28P:admin#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DES-3200-28P:admin#
```

31-16 disable address_binding trap_log

Description

This command is used to disable the IMPB traps and logs.

Format

disable address_binding trap_log

Parameters

None.

Restrictions

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

Example

To disable IMPB traps and logs:

```
DES-3200-28P:admin#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DES-3200-28P:admin#
```

31-17 config address_binding recover_learning

Description

This command is used to recover IMPB checking.

Format

config address_binding recover_learning ports [<portlist> | all]

Parameters

ports - Specify the list of ports that need to recover the IMPB check. **<portlist>** - Enter the list of port used here. **all** - Specify that all the ports will be used.

Restrictions

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

Example

To recover IMPB checking for ports 6 to 7:

```
DES-3200-28P:admin#config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

DES-3200-28P:admin#
```

31-18 debug address_binding

Description

This command is used to start the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

debug address_binding [event | dhcp | all] state [enable | disable]

Parameters

event - To print out the debug messages when IMPB module receives ARP/IP packets. **dhcp** - To print out the debug messages when the IMPB module receives the DHCP packets. **all** - Print out all debug messages.
state - This parameter configures the IMPB debug state to be enabled or disabled. **enable** - Specify that the state will be enabled. **disable** - Specify that the state will be disabled.

Restrictions

Only Administrator users can issue this command.

Example

To print out all debug IMPB messages:

```
DES-3200-28P:admin#debug address_binding all state enable
Command: debug address_binding all state enable

Success.

DES-3200-28P:admin#
```

31-19 no debug address_binding

Description

This command is used to stop the IMPB debug starting when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

no debug address_binding

Parameters

None.

Restrictions

Only Administrator users can issue this command.

Example

To stop IMPB debug: starting when the IMPB module receives an ARP/IP or DHCP packet:

```
DES-3200-28P:admin#no debug address_binding
Command: no debug address_binding

Success.

DES-3200-28P:admin#
```

Chapter 32 IPv6 Neighbor Discover Command List

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]
show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]
config ipv6 nd ns ipif <ipif_name 12> **retrans_time** <millisecond 0-4294967295>
show ipv6 nd {ipif <ipif_name 12>}

32-1 create ipv6 neighbor_cache

Description

This command is used to add a static neighbor on an IPv6 interface.

Format

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>

Parameters

ipif - Specify the interface's name. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
<ipv6addr> - The address of the neighbor.
<macaddr> - The MAC address of the neighbor.

Restrictions

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

Example

Create a static neighbor cache entry:

```
DES-3200-28P:admin#create ipv6 neighbor_cache ipif System 3ffc::1  00-01-02-03-
04-05
Command: create ipv6 neighbor_cache ipif System 3ffc::1  00-01-02-03-04-05

Success.

DES-3200-28P:admin#
```

32-2 delete ipv6 neighbor_cache

Description

This command is used to delete a neighbor cache entry or static neighbor cache entries from the address cache or all address cache entries on this IP interface. Both static and dynamic entries can be deleted.

Format

delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]

Parameters

ipif - Specify the IPv6 interface name. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long. **all** - Specify that all the interfaces will be used in this configuration.
<ipv6addr> - The neighbor's address.
static - Delete the static entry.
dynamic - Delete those dynamic entries.
all - All entries include static and dynamic entries will be deleted.

Restrictions

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

Example

Delete a neighbor cache.entry on IP interface "System":

```
DES-3200-28P:admin#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

DES-3200-28P:admin#
```

32-3 show ipv6 neighbor_cache

Description

This command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all entries, or all static entries.

Format

show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]

Parameters

ipif - Specify the IPv6 interface name

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long. **all** - Specify that all the interface will be displayed.
ipv6address - The neighbor's address. **<ipv6addr>** - Enter the IPv6 address here.
static - Static neighbor cache entry.
dynamic - Dynamic entries.
all - All entries include static and dynamic entries.

Restrictions

None

Example

Show all neighbor cache entries of IP interface "System":

```
DES-3200-28P:admin#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all


3FFC::1                                 State: Static
MAC Address : 00-01-02-03-04-05         Port : NA
Interface   : System                    VID  : 1

Total Entries: 1


DES-3200-28P:admin#
```

32-4 config ipv6 nd ns retrans_time

Description

This command is used to configure the IPv6 ND neighbor solicitation retransmit time, which is between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Format

config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>

Parameters

ipif - The IPv6 interface name **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
retrans_time - Neighbor solicitation's re-transmit timer in millisecond. **<millisecond 0-4294967295>** - Enter the re-transmit timer value here. This value must be between 0 and 4294967295 milliseconds.

Restrictions

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

Example

To configure the retrans_time of IPv6 ND neighbor solicitation:

```
DES-3200-28P:admin#config ipv6 nd ns ipif Zira retrans_time 1000000
Command: config ipv6 nd ns ipif Zira retrans_time 1000000

Success.

DES-3200-28P:admin#
```

32-5 show ipv6 nd

Description

This command is used to display information regarding neighbor detection on the Switch.

Format

show ipv6 nd {ipif <ipif_name 12>}

Parameters

ipif – (Optional) The name of the interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
If no IP interface is specified, it will show the IPv6 ND related configuration of all interfaces.

Restrictions

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

Example

To show IPv6 ND related configuration:

```
DES-3200-28P:admin#show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name            : System
NS Retransmit Time        : 0 (ms)

DES-3200-28P:admin#
```

Chapter 33 IPv6 Route Command List

create ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>}
delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]
show ipv6route

33-1 create ipv6route

Description

This command is used to create an IPv6 default route. If the next hop is a global address, it is not needed to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Format

create ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>}

Parameters

default - Specify the default route.
<ipif_name 12> - Specify the interface for the route. This name can be up to 12 characters long. **<ipv6addr>** - Specify the next hop address for this route.
<ipv6addr> - Specify the next hop address for this route.
<metric 1-65535> - (Optional) Enter the metric value here. The default setting is 1. This value must between 1 and 65535.

Restrictions

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

Example

To create and IPv6 route:

```
DES-3200-28P:admin#create ipv6route default System 3FFC::1
Command: create ipv6route default System 3FFC::1

Success.

DES-3200-28P:admin#
```

33-2 delete ipv6route

Description

This command is used to delete an IPv6 static route. If the next hop is a global address, it is not needed to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Format

delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]

Parameters

default - Specify the default route.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long. **<ipv6addr>** - Specify the next hop address for the default route.
<ipv6addr> - Specify the next hop address for the default route.
all - Specify that all static created routes will be deleted.

Restrictions

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

Example

Delete an IPv6 static route:

```
DES-3200-28P:admin#delete ipv6route default System 3FFC::1
Command: delete ipv6route default System 3FFC::1

Success.

DES-3200-28P:admin#
```

33-3 show ipv6route

Description

This command is used to display IPv6 routes.

Format

show ipv6route

Parameters

None.

Restrictions

None.

Example

Show all the IPv6 routes:

```
DES-3200-28P:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                              Protocol: Static  Metric: 1
Next Hop   : 3001::254                         IPIF    : System
Status     : Inactive

Total Entries: 1

DES-3200-28P:admin#
```

Chapter 34 Jumbo Frame Command List

enable jumbo_frame
disable jumbo_frame
show jumbo_frame

34-1 enable jumbo_frame

Description

This command is used to configure the jumbo frame setting as enable.

Format

enable jumbo_frame

Parameters

None.

Restrictions

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

Example

To enable the Jumbo frame:

```
DES-3200-28P:admin#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 12288 bytes.
Success.

DES-3200-28P:admin#
```

34-2 disable jumbo_frame

Description

This command is used to configure the jumbo frame setting as disable.

Format

disable jumbo_frame

Parameters

None.

Restrictions

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

Example

To disable the Jumbo frame:

```
DES-3200-28P:admin#disable jumbo_frame
Command: disable jumbo_frame

Success.

DES-3200-28P:admin#
```

34-3 show jumbo_frame

Description

This command is used to display the current configuration of jumbo frame.

Format

show jumbo_frame

Parameters

None.

Restrictions

None.

Example

To show the Jumbo frame:

```
DES-3200-28P:admin#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State  : Disabled
Maximum Frame Size : 1536 Bytes

DES-3200-28P:admin#
```

Chapter 35 Layer 2 Protocol Tunneling (L2PT) Command List

enable l2protocol_tunnel
disable l2protocol_tunnel
config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-65535>} | nni | none]
show l2protocol_tunnel {[uni | nni]}

35-1 enable l2protocol_tunnel

Description

This command is used to enable the Layer 2 protocol tunneling function.

Format

enable l2protocol_tunnel

Parameters

None.

Restrictions

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

Example

To enable the Layer 2 protocol tunneling function:

```
DES-3200-28P:admin#enable l2protocol_tunnel
Command: enable l2protocol_tunnel

Success.

DES-3200-28P:admin#
```

35-2 disable l2protocol_tunnel

Description

This command is used to disable the L2PT function globally on the Switch.

Format

disable l2protocol_tunnel

Parameters

None.

Restrictions

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

Example

To disable the Layer 2 protocol tunneling function:

```
DES-3200-28P:admin#disable l2protocol_tunnel
Command: disable l2protocol_tunnel

Success.

DES-3200-28P:admin#
```

35-3 config l2protocol_tunnel ports

Description

This command is used to configure Layer 2 protocol tunneling on ports. Layer 2 protocol tunneling is used to tunnel Layer 2 protocol packet. If a Layer 2 protocol is tunnel-enabled on an UNI, once received the PDU on this port, the multicast destination address of the PDU will be replaced by Layer 2 protocol tunneling multicast address. The Layer 2 protocol tunneling multicast address for STP is 01-05-5D-00-00-00, for GVRP is 01-05-5D-00-00-21, for Layer 2 protocols MAC 01-00-0C-CC-CC-CC is 01-05-5D-00-00-10 and for protocol MAC 01-00-0C-CC-CC-CD is 01-05-5D-00-00-11.

When QinQ is enabled, an S-TAG will be added to the Layer 2 PDU too. The S-TAG is assigned according QinQ VLAN configuration.

Format

config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-65535>} | nni | none]

Parameters

<portlist> - Specify a list of ports on which the Layer 2 protocol tunneling to be configured.
all – Specify to have all ports to be configured
type - Specify the type of the ports. **uni** - Specify the ports as UNI ports. **tunneled_protocol** - Specify tunneled protocols on the UNI ports. **stp** - Specify to use the STP protocol. **gvrp** - Specify to use the GVRP protocol. **protocol_mac** - Specify the destination MAC address of the L2 protocol packets that will tunneled on these UNI ports. **01-00-0C-CC-CC-CC** - Specify the MAC address as 01-00-0C-CC-CC-CC.

01-00-0C-CC-CC-CD - Specify the MAC address as 01-00-0C-CC-CC-CD.
all - All tunnel-abled Layer 2 protocols will be tunneled on the ports.
threshold - (Optional) Specify the drop threshold for packets-per-second accepted on the UNI ports. The ports drop the PDU if the protocol's threshold is exceeded.
<value 0-65535> - The range of the threshold value is 0 to 65535 (packet/second). The value 0 means no limit. By default, the value is 0.
nni - Specify the ports as NNI ports.
none - Disable tunnel on it.

Restrictions

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

Example

To configure the STP tunneling on ports 1-4:

```
DES-3200-28P:admin#config l2protocol_tunnel ports 1-4 type uni
tunneled_protocol stp
Command: config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp

Success.

DES-3200-28P:admin#
```

35-4 show l2protocol_tunnel

Description

This command is used to display Layer 2 protocol tunneling information.

Format

show l2protocol_tunnel {[uni | nni]}

Parameters

uni - (Optional) Specify to show UNI detail information, include tunneled and dropped PDU statistic.
nni - (Optional) Specify to show NNI detail information, include de-capsulated Layer 2 PDU statistic.

Restrictions

None.

Example

To show Layer 2 protocol tunneling information summary:

```
DES-3200-28P:admin#show l2protocol_tunnel
Command: show l2protocol_tunnel

Global State : Enabled
UNI Ports    : 1-4
NNI Ports    :

DES-3200-28P:admin#
```

To show Layer 2 protocol tunneling information summary:

```
DES-3200-28P:admin#show l2protocol_tunnel uni
Command: show l2protocol_tunnel uni

 UNI   Tunneled           Threshold
 Port  Protocol           (packet/sec)
 ----  -----------------  ------------
 1     STP                0
 2     STP                0
 3     STP                0
 4     STP                0

DES-3200-28P:admin#
```

Chapter 36 Link Aggregation Command List

create link_aggregation group_id <value> {type [lacp | static]}
delete link_aggregation group_id <value>
config link_aggregation group_id <value> {master_port <port> | ports <portlist> | state [enable | disable]
config link_aggregation algorithm [mac_source | mac_destination|mac_source_dest | ip_source | ip_destination | ip_source_dest]
show link_aggregation {group_id <value> | algorithm}
config lacp_port <portlist> mode [active | passive]
show lacp_port <portlist>

36-1 create link_aggregation group_id

Description

This command is used to create a link aggregation group on the Switch.

Format

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

Parameters

<value > - Enter the group ID value here.
type - (Optional) Specify the group type is belong to static or LACP. If type is not specified, the default is static type. **lacp** - Specify to use LACP as the group type. **static** - Specify to use static as the group type.

Restrictions

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

Example

To create link aggregation group:

```
DES-3200-28P:admin#create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success.

DES-3200-28P:admin#
```

36-2 delete link_aggregation group_id

Description

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

Format

delete link_aggregation group_id <value>

Parameters

group_id - Specify the group id. The number of link aggregation groups is project dependency. The group number identifies each of the groups. **<value>** - Enter the group ID value here.

Restrictions

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

Example

To delete link aggregation group:

```
DES-3200-28P:admin#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

DES-3200-28P:admin#
```

36-3 config link_aggregation group_id

Description

This command is used to configure a previously created link aggregation group.

Format

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

Parameters

group_id - Specify the group id. The group number identifies each of the groups. **<value>** - Enter the group ID value here. This value must be between 1 and 32.
master_port - (Optional) Master port ID. Specify which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. **<port>** - Enter the master port number here.
ports - (Optional) Specify a range of ports that will belong to the link aggregation group. **<portlist>** - Enter the list of port used for the configuration here.
state - (Optional) Enable or disable the specified link aggregation group. If not specified, the group will keep the previous state, the default state is disabled. If configure LACP group, the

ports' state machine will start. **enable** - Enable the specified link aggregation group. **disable** - Disable the specified link aggregation group.

Restrictions

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

Example

To define a load-sharing group of ports:

```
DES-3200-28P:admin#config link_aggregation group_id 1 master_port 5 ports 5-7
Command: config link_aggregation group_id 1 master_port 5 ports 5-7

Success.

DES-3200-28P:admin#
```

36-4 config link_aggregation algorithm

Description

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

Format

config link_aggregation algorithm [mac_source | mac_destination|mac_source_dest | ip_source | ip_destination | ip_source_dest]

Parameters

mac_source - Indicates that the Switch should examine the MAC source address.
mac_destination - Indicates that the Switch should examine the MAC destination address.
mac_source_dest - Indicates that the Switch should examine the MAC source and destination address.
ip_source - Indicates that the Switch should examine the IP source address.
ip_destination - Indicates that the Switch should examine the IP destination address.
ip_source_dest - Indicates that the Switch should examine the IP source address and destination address.

Restrictions

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

Example

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

```
DES-3200-28P:admin#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3200-28P:admin#
```

36-5 show link_aggregation

Description

This command is used to display the current link aggregation configuration on the Switch.

Format

show link_aggregation {group_id <value> | algorithm}

Parameters

group_id - (Optional) Specify the group id. The group number identifies each of the groups. **<value >** - Enter the group ID value here.
algorithm - (Optional) Allows you to specify the display of link aggregation by the algorithm in use by that group.
If no parameter specified, system will display all link aggregation information.

Restrictions

None.

Example

Link aggregation group enable:

```
DES-3200-28P:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 5
Member Port   : 5-7
Active Port   :
Status        : Enabled
Flooding Port : 7

Total Entries : 1

DES-3200-28P:admin#
```

Link aggregation group enable and no member linkup:

```
DES-3200-28P:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 5
Member Port   : 5-7
Active Port   :
Status        : Enabled
Flooding Port :

Total Entries : 1

DES-3200-28P:admin#
```

Link aggregation group disabled:

```
DES-3200-28P:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 5
Member Port   : 5-7
Active Port   :
Status        : Disabled
Flooding Port : 7

Total Entries : 1

DES-3200-28P:admin#
```

36-6 config lacp_port

Description

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

Format

config lacp_port <portlist> mode [active | passive]

Parameters

lacp_port - Specify a range of ports to be configured. **<portlist>** - Enter the list of port used for the configuration here.
mode - Specify the LACP mode used. **active** - Specify to set the LACP mode as active.

passive - Specify to set the LACP mode as passive.

Restrictions

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

Example

To config port LACP mode:

```
DES-3200-28P:admin#config lacp_port 1-12 mode active
command: config lacp_port 1-12 mode active

Success.

DES-3200-28P:admin#
```

36-7 show lacp_port

Description

This command is used to display the current mode of LACP of the ports.

Format

show lacp_port <portlist>

Parameters

lacp_port - Specify a range of ports to be configured. **<portlist>** - Enter the list of ports used for this configuration here.
If no parameter specified, the system will display current LACP and all port status.

Restrictions

None.

Example

To show port lacp mode:

```
DES-3200-28P:admin#show lacp_port
Command: show lacp_port

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

DES-3200-28P:admin#
```

Chapter 37 Link Layer Discovery Protocol (LLDP) Command List

enable lldp
disable lldp
config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]
config lldp notification_interval <sec 5-3600>
config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable| disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>][enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp }][enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | power_via_mdi|maximum_frame_size}][enable | disable]]
config lldp forward_message [enable | disable]
show lldp
show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}
show lldp ports {<portlist>}
show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp statistics
show lldp statistics ports {<portlist>}

37-1 enable lldp

Description

This command is used to globally enable the LLDP function.

When this function is enabled, the Switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per-port LLDP setting.

For the advertisement of LLDP packets, the Switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the Switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. The default state for LLDP is disabled.

Format

enable lldp

Parameters

None.

Restrictions

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

Example

To enable LLDP:

```
DES-3200-28P:admin#enable lldp
Command: enable lldp

Success.

DES-3200-28P:admin#
```

37-2 disable lldp

Description

This command is used to stop sending and receiving of LLDP advertisement packet.

Format

disable lldp

Parameters

None.

Restrictions

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

Example

To disable LLDP:

```
DES-3200-28P:admin#disable lldp
Command: disable lldp

Success.

DES-3200-28P:admin#
```

37-3 config lldp

Description

This command is used to change the packet transmission interval.

Format

config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]

Parameters

message_tx_interval - Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The default setting 30 seconds. **<sec 5-32768>** - Enter the message transmit interval value here. This value must be between 5 and 32768 seconds.
message_tx_hold_multiplier - Specify to configure the message hold multiplier. The default setting 4. **<2-10>** - Enter the message transmit hold multiplier value here. This value must be between 2 and 10.
tx_delay - Specify the minimum interval between sending of LLDP messages due to constantly change of MIB content. The default setting 2 seconds. **<sec 1-8192>** - Enter the transmit delay value here. This value must be between 1 and 8192 seconds.
reinit_delay - Specify the the minimum time of reinitialization delay interval. The default setting 2 seconds. **<sec 1-10>** - Enter the re-initiate delay value here. This value must be between 1 and 10 seconds.

Restrictions

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

Example

To change the packet transmission interval:

```
DES-3200-28P:admin#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DES-3200-28P:admin#
```

37-4 config lldp notification_interval

Description

This command is used to configure the timer of notification interval for sending notification to configured SNMP trap receiver(s).

Format

config lldp notification_interval <sec 5-3600>

Parameters

notification_interval - Specify the timer of notification interval for sending notification to configured SNMP trap receiver(s). The default setting is 5 seconds.

<sec 5-3600> - Enter the notification interval value here. This value must be between 5 and 3600 seconds.

Restrictions

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

Example

To changes the notification interval to 10 second:

```
DES-3200-28P:admin#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DES-3200-28P:admin#
```

37-5 config lldp ports

Description

This command is used to configure each port for sending a notification to configure the SNMP trap receiver(s).

Format

config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable| disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>][enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp }][enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | power_via_mdi|maximum_frame_size}][enable | disable]]

Parameters

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

all - Specify that all the ports will be used for this configuration.

notification - Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.
- **enable** - Specify that the SNMP trap notification of LLDP data changes detected will be enabled.
- **disable** - Specify that the SNMP trap notification of LLDP data changes detected will be disabled.

admin_status - Specify the per-port transmit and receive modes.
- **tx_only** - Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices.
- **rx_only** - Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors.
- **tx_and_rx** - Configure the specified port(s) to both transmit and receive LLDP packets.
- **disable** - Disable LLDP packet transmit and receive on the specified port(s).

mgt_addr - Specify the management address used.
- **ipv4** - Specify the IPv4 address used.
  - **<ipaddr>** - Enter the IP address used for this configuration here.
- **ipv6** - Specify the IPv6 address used.
  - **<ipv6addr>** - Enter the IPv6 address used for this configuration here.
- **enable** - Specify that the advertising indicated management address instance will be enabled.
- **disable** - Specify that the advertising indicated management address instance will be disabled.

basic_tlvs - Specify the basic TLV data types used from outbound LLDP advertisements.
- **all** - (Optional) Specify that all the basic TLV data types will be used.
- **port_description** - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled.
- **system_name** - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit 'System Name TLV'. The default state is disabled.
- **system_description** - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit 'System Description TLV'. The default state is disabled.
- **system_capabilities** - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.
- **enable** - Specify that the basic TLV data types used from outbound LLDP advertisements will be enabled.
- **disable** - Specify that the basic TLV data types used from outbound LLDP advertisements will be disabled.

dot1_tlv_pvid - This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disable.
- **enable** - Specify that the Dot1 TLV PVID option will be enabled.
- **disable** - Specify that the Dot1 TLV PVID option will be disabled.

dot1_tlv_protocol_vid - This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disable.
- **vlan** - Specify the VLAN used for this configuration.
  - **all** - Specify that all the configured VLANs will be used for this configuration.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
  - **vlanid** - Specify the VLAN ID used for this configuration.
    - **<vlanid_list>** - Enter the ID of the VLAN here.
- **enable** - Specify that the Dot1 TLV protocol VID will be enabled.
- **disable** - Specify that the Dot1 TLV protocol VID will be disabled.

dot1_tlv_vlan_name - This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs. those enabled VLAN ID will be advertised. The default state is disable.
- **vlan** - Specify the VLAN used for this configuration.
  - **all** - Specify that all the configured VLANs will be used for this configuration.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
  - **vlanid** - Specify the VLAN ID used for this configuration.
    - **<vlanid_list>** - Enter the ID of the VLAN here.
- **enable** - Specify that the Dot1 TLV VLAN name will be enabled.
- **disable** - Specify that the Dot1 TLV VLAN name will be disabled.

dot1_tlv_protocol_identity - This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised. The default state is disabled.
- **all** - Specify that all the vendor proprietary protocols will be advertised.

eapol - (Optional) Specify that the EAPOL protocol will be advertised.
lacp - (Optional) Specify that the LACP protocol will be advertised.
gvrp - (Optional) Specify that the GVRP protocol will be advertised.
stp - (Optional) Specify that the STP protocol will be advertised.
enable - Specify that the protocol identity TLV according to the protocol specified will be adverstised.
disable - Specify that the protocol identity TLV according to the protocol specified will not be adverstised.

dot3_tlvs - Specify that the IEEE 802.3 specific TLV data type will be configured.
all - (Optional) Specify that all the IEEE 802.3 specific TLV data type will be used.
mac_phy_configuration_status - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supported the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disabled.
link_aggregation - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Link Aggregation TLV'. This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in a aggregated link, and the aggregated port ID. The default state is disabled.
power_via_mdi - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Power via MDI TLV'. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station. The default state is disabled.
maximum_frame_size - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is disabled.
enable - Specify that the IEEE 802.3 specific TLV data type selected will be advertised.
disable - Specify that the IEEE 802.3 specific TLV data type selected will be not advertised.

Restrictions

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

Example

To enable SNMP notifications from port 1-5:

```
DES-3200-28P:admin#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DES-3200-28P:admin#
```

To configure port 1-5 to transmit and receive:

```
DES-3200-28P:admin#config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DES-3200-28P:admin#
```

To enable ports 1-2 for manage address entry:

```
DES-3200-28P:admin#config lldp ports 1-2 mgt_addr ipv4 10.90.90.90 enable
Command: config lldp ports 1-2 mgt_addr ipv4 10.90.90.90 enable

Success.

DES-3200-28P:admin#
```

To configure exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28P:admin#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DES-3200-28P:admin#
```

To configure exclude the vlan nameTLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28P:admin#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DES-3200-28P:admin#
```

To configure exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28P:admin#config lldp ports all dot1_tlv_protocol_vid vlanid 1-3
enable
Command: config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable

Success.

DES-3200-28P:admin#
```

To configure exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28P:admin#config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

DES-3200-28P:admin#
```

To configure exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28P:admin#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DES-3200-28P:admin#
```

To configure exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28P:admin#config lldp ports all dot3_tlvs mac_phy_configuration_status
enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

DES-3200-28P:admin#
```

37-6 config lldp forward_ message

Description

This command is used to configure forwarding of LLDP PDU packet when LLDP is disabled.

Format

config lldp forward_message [enable | disable]

Parameters

None.

Restrictions

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

Example

To configure LLDP to forward LLDP PDUs:

```
DES-3200-28P:admin#config lldp forward_message  enable
Command: config lldp forward_message enable

Success.

DES-3200-28P:admin#
```

37-7 show lldp

Description

This command is used to display the Switch's general LLDP configuration status.

Format

show lldp

Parameters

None.

Restrictions

None.

Example

To display the LLDP system level configuration status:

```
DES-3200-28P:admin#show lldp
Command: show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 00-01-02-03-04-00
    System Name               :
    System Description        : Fast Ethernet Switch
    System Capabilities       : Repeater, Bridge

LLDP Configurations
    LLDP Status               : Enabled
    LLDP Forward Status       : Enabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
    TX Delay                  : 2
    Notification Interval     : 10

DES-3200-28P:admin#
```

37-8 show lldp mgt_addr

Description

This command is used to display the LLDP management address information.

Format

show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}

Parameters

ipv4 - (Optional) Specify the IPv4 address used for the display. **<ipaddr>** - Enter the IPv4 address used for this configuration here.

ipv6 - (Optional) Specify the IPv6 address used for the display. **<ipv6addr>** - Enter the IPv6 address used for this configuration here.

Restrictions

None.

Example

To display management address information:

```
DES-3200-28P:admin#show lldp mgt_addr ipv4 10.90.90.90
Command: show lldp mgt_addr ipv4 10.90.90.90

Address 1 :
-----------------------------------------------
    Subtype                           : IPv4
    Address                           : 10.90.90.90
    IF Type                           : IfIndex
    OID                               : 1.3.6.1.4.1.171.10.113.8.1
    Advertising Ports                 : 1-2,5

DES-3200-28P:admin#
```

37-9 show lldp ports

Description

This command is used to display the LLDP per port configuration for advertisement options.

Format

show lldp ports {<portlist>}

Parameters

<portlist> - (Optional) Specify a range of ports to be displayed. If the port list is not specified, information for all the ports will be displayed.

Restrictions

None.

Example

To display the LLDP port 1 TLV option configuration:

```
DES-3200-28P:admin#show lldp ports  1
Command: show lldp ports 1

Port ID                 : 1
------------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Enabled
Advertised TLVs Option  :
    Port Description                                    Disabled
    System Name                                         Enabled
    System Description                                  Disabled
    System Capabilities                                 Disabled
    Enabled Management Address
        10.90.90.90
    Port VLAN ID                                        Enabled
    Enabled Port_and_Protocol_VLAN_ID
        1, 2, 3
    Enabled VLAN Name
        1-3
    Enabled Protocol_Identity
        (None)
    MAC/PHY Configuration/Status                        Disabled
    Power Via MDI                                       Disabled
    Link Aggregation                                    Disabled
    Maximum Frame Size                                  Disabled


DES-3200-28P:admin#
```

37-10 show lldp local_ports

Description

This command is used to display the per-port information currently available for populating outbound LLDP advertisements.

Format

show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}

Parameters

<portlist> - (Optional) Specify a range of ports to be configured. When port list is not specified, information for all ports will be displayed.
mode - (Optional) Specify the display mode. **brief** - Display the information in brief mode. **normal** - Display the information in normal mode. This is the default display mode. **detailed** - Display the information in detailed mode.

Restrictions

None.

Example

To display outbound LLDP advertisements for port 1 in detailed mode. Port description on the display should use the same value as ifDescr.

```
DES-3200-28P:admin#show lldp local_ports 1 mode detailed
Command: show lldp local_ports 1 mode detailed


Port ID : 1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : 1
Port Description                         : D-Link DES-3200-28P R4.00.020 P
                                           ort 1
Port PVID                                : 1
Management Address Count                 : 1
        Subtype                          : IPv4
        Address                          : 10.90.90.90
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.171.10.113.8.1

PPVID Entries Count                      : 0
    (None)
VLAN Name Entries Count                  : 1
    Entry 1 :
        VLAN ID                          : 1
        VLAN Name                        : default

Protocol Identity Entries Count          : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display outbound LLDP advertisements for port 1 in normal mode:

```
DES-3200-28P:admin#show lldp local_ports 1 mode normal
Command: show lldp local_ports 1 mode normal


Port ID : 1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : 1
Port Description                         : D-Link DES-3200-28P R4.00.020 P
                                           ort 1
Port PVID                                : 1
Management Address Count                 : 1
PPVID Entries Count                      : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status             : (See Detail)
Power Via MDI                            : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1536

DES-3200-28P:admin#
```

To display outbound LLDP advertisements for port 1 in brief mode:

```
DES-3200-28P:admin#show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief


Port ID : 1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : 1
Port Description                         : D-Link DES-3200-28P R4.00.020 P
                                           ort 1

DES-3200-28P:admin#
```

37-11 show lldp remote_ports

Description

This command is used to display the information learned from the neighbor parameters.

Format

show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}

Parameters

<portlist> - (Optional) Specify a range of ports to be configured. When port list is not specified, information for all ports will be displayed.
mode – (Optional) Specify to display the information in various modes.

brief - Display the information in brief mode.
normal - Display the information in normal mode. This is the default display mode.
detailed - Display the information in detailed mode.

Restrictions

None.

Example

To display remote table in brief mode:

```
DES-3200-28P:admin#show lldp remote_ports 3 mode brief
Command: show lldp remote_ports 3 mode brief

Port ID : 3
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                        : MAC Address
    Chassis ID                                : 00-12-13-04-05-00
    Port ID Subtype                           : MAC Address
    Port ID                                   : 00-12-13-04-05-03
    Port Description                          : D-Link DES-3200-28P R4.00.020
Po
                                                rt 3

DES-3200-28P:admin#
```

To display remote table in normal mode:

```
DES-3200-28P:admin# show lldp remote_ports 3 mode normal
Command: show lldp remote_ports 3 mode normal

Port ID : 3
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-12-13-04-05-00
    Port ID Subtype                             : MAC Address
    Port ID                                     : 00-12-13-04-05-03
    Port Description                            : D-Link DES-3200-28P R4.00.020
Po
                                                  rt 3
    System Name                                 :
    System Description                          : Fast Ethernet Switch
    System Capabilities                         : Repeater, Bridge
    Management Address Count                    : 1
    Port PVID                                   : 1
    PPVID Entries Count                         : 0
    VLAN Name Entries Count                     : 0
    Protocol ID Entries Count                   : 0
    MAC/PHY Configuration/Status                : (See Detail)
    Power Via MDI                               : (None)
    Link Aggregation                            : (See Detail)
    Maximum Frame Size                          : 1536
    Unknown TLVs Count                          : 0


DES-3200-28P:admin#
```

To display remote table in detailed mode:

```
DES-3200-28P:admin# show lldp remote_ports 3 mode detailed
Command: show lldp remote_ports 3 mode detailed

Port ID : 3
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-12-13-04-05-00
    Port ID Subtype                             : MAC Address
    Port ID                                     : 00-12-13-04-05-03
    Port Description                            : D-Link DES-3200-28P R4.00.020
Po
                                                  rt 3
    System Name                                 :
    System Description                          : Fast Ethernet Switch
    System Capabilities                         : Repeater, Bridge
    Management Address Count                    : 1
        Entry 1 :
            Subtype                             : IPv4
            Address                             : 10.90.90.90
            IF Type                             : IfIndex
            OID                                 : 1.3.6.1.4.1.171.10.113.9.1

    Port PVID                                   : 1

    PPVID Entries Count                         : 0
        (None)

    VLAN Name Entries Count                     : 0
        (None)

    Protocol ID Entries Count                   : 0
        (None)

    MAC/PHY Configuration/Status                :
        Auto-Negotiation Support                : Supported
        Auto-Negotiation Status                 : Enabled
        Auto-Negotiation Advertised Capability  : 6c00(hex)
        Auto-Negotiation Operational MAU Type   : 0010(hex)

    Power Via MDI                               : (None)
    Link Aggregation                            :
        Aggregation Capability                  : Aggregated
        Aggregation Status                      : Not Currently in Aggregation
        Aggregation Port ID                     : 0

    Maximum Frame Size                          : 1536
    Unknown TLVs Count                          : 0
        (None)

DES-3200-28P:admin#
```

37-12 show lldp statistics

Description

This command is used to display an overview of neighbor detection activity on the Switch.

Format

show lldp statistics

Parameters

None.

Restrictions

None.

Example

To display global statistics information:

```
DES-3200-28P:admin#show lldp statistics
Command: show lldp statistics

Last Change Time       : 1792
Number of Table Insert : 0
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0

DES-3200-28P:admin#
```

37-13 show lldp statistics ports

Description

This command is used to display per-port LLDP statistics

Format

show lldp statistics ports {<portlist>}

Parameters

<portlist> - (Optional) Specify a range of ports to be configured. When port list is not specified, information for all ports will be displayed.

Restrictions

None.

Example

To display statistics information of port 1:

```
DES-3200-28P:admin#show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
-----------------------------------------------
    LLDPStatsTXPortFramesTotal           : 23
    LLDPStatsRXPortFramesDiscardedTotal  : 0
    LLDPStatsRXPortFramesErrors          : 0
    LLDPStatsRXPortFramesTotal           : 0
    LLDPStatsRXPortTLVsDiscardedTotal    : 0
    LLDPStatsRXPortTLVsUnrecognizedTotal : 0
    LLDPStatsRXPortAgeoutsTotal          : 0

DES-3200-28P:admin#
```

Chapter 38 Loop Back Detection (LBD) Command List

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}
config loopdetect ports [<portlist> | all] state [enable | disable]
enable loopdetect
disable loopdetect
show loopdetect
show loopdetect ports {<portlist>}
config loopdetect trap [none | loop_detected | loop_cleared | both]
config loopdetect log state [enable | disable]

38-1 config loopdetect

Description

This command is used to setup the loop-back detection function (LBD) for the entire Switch.

Format

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}

Parameters

recover_timer - (Optional) The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check before determining that the loop status has gone. The valid range is from 60 to 1000000. 0 is a special value that specifies that the auto-recovery mechanism should be disabled. When the auto-recovery mechanism is disabled, a user would need to manually recover a disabled port. The default value for the recover timer is 60 seconds. **<value 0>** - 0 is a special value that specifies that the auto-recovery mechanism should be disabled. When the auto-recovery mechanism is disabled, a user would need to manually recover a disabled port. **<sec 60-1000000>** - Enter the recovery timer value here. This value must be between 60 and 1000000 seconds.
interval - (Optional) The time interval (in seconds) that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The default setting is 10 seconds. The valid range is from 1 to 32767 seconds. **<sec - 1-32767>** - Enter the time interval value here. This value must be between 1 and 32767 seconds.
mode - (Optional) Specify the loop-detection operation mode. In port-based mode, the port will be shut down (disabled) when loop has been detected In VLAN-based mode, the port cannot process the packets of the VLAN that has detected the loop. **port-based** - Specify that the loop-detection operation mode will be set to port-based mode. **vlan-based** - Specify that the loop-detection operation mode will be set to vlan-based mode.

Restrictions

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

Example

To set the auto-recover time to 0, which disables the auto-recovery mechanism, the interval to 20 seconds and specify VLAN-based mode:

```
DES-3200-28P:admin#config loopdetect recover_timer 0 interval 20 mode vlan-
based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

DES-3200-28P:admin#
```

38-2 config loopdetect ports

Description

This command is used to setup the loop-back detection function for the interfaces on the Switch.

Format

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

Parameters

ports - Specify the range of ports that LBD will be configured on. **<portlist>** - Enter a list of ports **all** - To set all ports in the system, you may use the “all” parameter.
state - Specify whether the LBD function should be enabled or disabled on the ports specified in the port list. The default state is disabled. **enable** - Specify to enable the LBD function. **disable** - Specify to disable the LBD function.

Restrictions

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

Example

To enable the LBD function on ports 1-5:

```
DES-3200-28P:admin#config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DES-3200-28P:admin#
```

38-3 enable loopdetect

Description

This command is used to enable the LBD function globally on the Switch. The default state is disabled.

Format

enable loopdetect

Parameters

None.

Restrictions

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

Example

To enable the LBD function globally:

```
DES-3200-28P:admin#enable loopdetect
Command: enable loopdetect

Success.

DES-3200-28P:admin#
```

38-4 disable loopdetect

Description

This command is used to disable the LBD function globally on the Switch.

Format

disable loopdetect

Parameters

None.

Restrictions

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

Example

To disable the LBD function globally:

```
DES-3200-28P:admin#disable loopdetect
Command: disable loopdetect

Success.

DES-3200-28P:admin#
```

38-5 show loopdetect

Description

This command is used to display the LBD global configuration.

Format

show loopdetect

Parameters

None.

Restrictions

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

Example

To show the LBD global settings:

```
DES-3200-28P:admin#show loopdetect
Command: show loopdetect

 LBD Global Settings
 ---------------------------
 Status         : Disabled
 Mode           : Port-based
 Interval       : 10 sec
 Recover Time   : 60 sec
 Trap State     : None
 Log State      : Enabled

DES-3200-28P:admin#
```

38-6 show loopdetect ports

Description

This command is used to display the LBD per-port configuration.

Format

show loopdetect ports {<portlist>}

Parameters

ports - Specify the range of member ports that will display the LBD settings. **<portlist>** - Enter the list of port to be configured here.
If no port is specified, the configuration for all ports will be displayed.

Restrictions

None.

Example

To show the LBD settings on ports 1-9:

```
DES-3200-28P:admin#show loopdetect  ports 1-9
Command: show loopdetect  ports 1-9

Port   Loopdetect State    Loop Status
------ ----------------- ----------
1      Enabled            Normal
2      Enabled            Normal
3      Enabled            Normal
4      Enabled            Normal
5      Enabled            Loop!
6      Enabled            Normal
7      Enabled            Loop!
8      Enabled            Normal
9      Enabled            Normal

DES-3200-28P:admin#
```

38-7 config loopdetect trap

Description

This command is used to configure the trap modes for LBD.

Format

config loopdetect trap [none | loop_detected | loop_cleared | both]

Parameters

none - There is no trap in the LBD function.
loop_detected - Trap will only be sent when the loop condition is detected.
loop_cleared - Trap will only be sent when the loop condition is cleared.
both - Trap will either be sent when the loop condition is detected or cleared.

Restrictions

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

Example

To specify that traps will be sent when the loop condition is detected or cleared:

```
DES-3200-28P:admin#config loopdetect trap both
Command: config loopdetect trap both

Success.

DES-3200-28P:admin#
```

38-8 config loopdetect log

Description

This command is used to configure the log state for LBD. The default value is enabled.

Format

config loopdetect log state [enable | disable]

Parameters

state - Specify the state of the LBD log feature. **enable** - Enable the LBD log feature. **disable** - Disable the LBD log feature. All LBD-related logs will not be recorded.

Restrictions

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

Example

To enable the log state for LBD:

```
DES-3200-28P:admin#config loopdetect log state enable
Command: config loopdetect log state enable

Success.

DES-3200-28P:admin#
```

Chapter 39 MAC Notification Command List

enable mac_notification
disable mac_notification
config mac_notification {interval <sec 1-2147483647> | historysize <int 1-500>}
config mac_notification ports [<portlist> | all] [enable | disable]
show mac_notification
show mac_notification ports {<portlist>}

39-1 enable mac_notification

Description

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

Format

enable mac_notification

Parameters

None.

Restrictions

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

Example

To enable mac_notification function:

```
DES-3200-28P:admin#enable mac_notification
Command: enable mac_notification

Success.

DES-3200-28P:admin#
```

39-2 disable mac_notification

Description

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

Format

disable mac_notification

Parameters

None.

Restrictions

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

Example

To disable mac_notification function:

```
DES-3200-28P:admin#disable mac_notification
Command: disable mac_notification

Success.

DES-3200-28P:admin#
```

39-3 config mac_notification

Description

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

Format

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

Parameters

interval - (Optional) The time in seconds between notifications. **<sec 1-2147483647>** - Enter the interval time here. This value must be between 1 and 2147483647 seconds.
historysize - (Optional) This is maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified. **<int 1-500>** - Enter the history log size here. This value must be between 1 and 500.

Restrictions

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

Example

To config the Switch's Mac address table notification global settings:

```
DES-3200-28P:admin#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DES-3200-28P:admin#
```

39-4 config mac_notification ports

Description

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

Format

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

Parameters

<portlist> - Enter a list of ports used for the configuration here. **all** - Specify that all the ports will be used for this configuration.
enable - Enable the port's MAC address table notification. **disable** - Disable the port's MAC address table notification.

Restrictions

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

Example

To enable 7th port's mac address table notification:

```
DES-3200-28P:admin#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-3200-28P:admin#
```

39-5 show mac_notification

Description

This command is used to display the Switch's Mac address table notification global settings.

Format

show mac_notification

Parameters

None.

Restrictions

None.

Example

To show the Switch's Mac address table notification global settings:

```
DES-3200-28P:admin#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State        : Disabled
Interval     : 1
History Size : 1

DES-3200-28P:admin#
```

39-6 show mac_notification ports

Description

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

Format

show mac_notification ports {<portlist>}

Parameters

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

Restrictions

None.

Example

To display all port's Mac address table notification status settings:

```
DES-3200-28P:admin#show mac_notification ports
Command: show mac_notification ports

Port    MAC Address Table Notification State
------  ------------------------------------
1                   Disabled
2                   Disabled
3                   Disabled
4                   Disabled
5                   Disabled
6                   Disabled
7                   Disabled
8                   Disabled
9                   Disabled
10                  Disabled
11                  Disabled
12                  Disabled
13                  Disabled
14                  Disabled
15                  Disabled
16                  Disabled
17                  Disabled
18                  Disabled
19                  Disabled
20                  Disabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Chapter 40 MAC-based Access Control Command List

enable mac_based_access_control
disable mac_based_access_control
config mac_based_access_control password <passwd 16>
config mac_based_access_control method [local | radius]
config mac_based_access_control guest_vlan ports <portlist>
config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-1000> | no_limit]}(1)
create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]
create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid < vlanid 1-4094>]}
config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)
show mac_based_access_control {ports {<portlist>}}
show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
show mac_based_access_control auth_state ports {<portlist>}
config mac_based_access_control max_users [<value 1-1000> | no_limit]
config mac_based_access_control trap state [enable | disable]
config mac_based_access_control log state [enable | disable]

40-1 enable mac_based_access_control

Description

This command is used to enable MAC-based Access Control.

Format

enable mac_based_access_control

Parameters

None.

Restrictions

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

Example

To enable the MAC-based Access Control global state:

```
DES-3200-28P:admin#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DES-3200-28P:admin#
```

40-2 disable mac_based_access_control

Description

This command is used to disable MAC-based Access Control.

Format

disable mac_based_access_control

Parameters

None.

Restrictions

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

Example

To disable the MAC-based Access Control global state:

```
DES-3200-28P:admin#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DES-3200-28P:admin#
```

40-3 config mac_based_access_control password

Description

This command is used to configure the RADIUS authentication password for MAC-based Access Control.

Format

config mac_based_access_control password <passwd 16>

Parameters

password - In RADIUS mode, the Switch will communicate with the RADIUS server using this password. The maximum length of the key is 16. **<password>** - Enter the password used here. The default password is “default”.

Restrictions

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

Example

To set the MAC-based Access Control password:

```
DES-3200-28P:admin#config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

DES-3200-28P:admin#
```

40-4 config mac_based_access_control method

Description

This command is used to configure the MAC-based Access Control authentication method.

Format

config mac_based_access_control method [local | radius]

Parameters

local - Specify to authenticate via the local database. **radius** - Specify to authenticate via a RADIUS server.

Restrictions

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

Example

To set the MAC-based Access Control authentication method as local:

```
DES-3200-28P:admin#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DES-3200-28P:admin#
```

40-5 config mac_based_access_control guest_vlan

Description

This command is used to assign a specified port list to the MAC-based Access Control guest VLAN. Ports that are not contained in port list will be removed from the MAC-based Access Control guest VLAN.

For detailed information on the operation of MAC-based Access Control guest VLANs, please see the description for the “config mac_based_access_control ports” command.

Format

config mac_based_access_control guest_vlan ports <portlist>

Parameters

ports - Specify MAC-based Access Control guest VLAN membership. **<portlist>** - Enter the list of port used for this configuration here.

Restrictions

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

Example

To set the MAC-based Access Control guest VLAN membership:

```
DES-3200-28P:admin#config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

DES-3200-28P:admin#
```

40-6 config mac_based_access_control ports

Description

This command is used to configure MAC-based Access Control port’s setting.

When the MAC-based Access Control function is enabled for a port and the port is not a MAC-based Access Control guest VLAN member, the user who is attached to this port will not be forwarded unless the user passes the authentication.

- A user that does not pass the authentication will not be serviced by the Switch.
- If the user passes the authentication, the user will be able to forward traffic operated under the assigned VLAN.

When the MAC-based Access Control function is enabled for a port, and the port is a MAC-based Access Control guest VLAN member, the port(s) will be removed from the original VLAN(s) member ports, and added to MAC-based Access Control guest VLAN member ports.

- Before the authentication process starts, the user is able to forward traffic under the guest VLAN.
- After the authentication process, the user will be able to access the assigned VLAN.

If the port authorize mode is port based mode, when the port has been moved to the authorized VLAN, the subsequent users will not be authenticated again. They will operate in the current authorized VLAN.

If the port authorize mode is host based mode, then each user will be authorized individually and be capable of getting its own assigned VLAN.

If port's block time is set to" infinite", it means that a failed authentication client will never be blocked. Block time will be set to "0".

Format

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-1000> | no_limit]}(1)

Parameters

ports - Specify a range of ports for configuring the MAC-based Access Control function parameters. **<portlist>** - Enter the list of port used for this configuration here. **all** - Specify all existed ports of switch for configuring the MAC-based Access Control function parameters.
state - (Optional) Specify whether the port's MAC-based Access Control function is enabled or disabled. **enable** - Specify that the port's MAC-based Access Control states will be enabled. **disable** - Specify that the port's MAC-based Access Control states will be disabled.
mode - (Optional) Specify the MAC-based access control port mode used. **port_based** - Specify that the MAC-based access control port mode will be set to port-based. **host_based** - Specify that the MAC-based access control port mode will be set to host-based.
aging_time - (Optional) A time period during which an authenticated host will be kept in an authenticated state. When the aging time has timed-out, the host will be moved back to unauthenticated state. **infinite** - If the aging time is set to infinite, it means that authorized clients will not be aged out automatically. **<min 1-1440>** - Enter the aging time value here. This value must be between 1 and 1440 minutes.
block_time - (Optional) If a host fails to pass the authentication, the next authentication will not start within the block time unless the user clears the entry state manually. If the block time is set to 0, it means do not block the client that failed authentication. **<sec 0-300>** -Enter the block time value here. This value must be between 0 and 300 seconds.
max_users - (Optional) Specify maximum number of users per port. **<value 1-1000>** - Enter the maximum number of users per port here. This value must be between 1 and 1000. **no_limit** - Specify to not limit the maximum number of users on the port. The default value is 128.

Restrictions

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

Example

To configure an unlimited number of maximum users for MAC-based Access Control on ports 1 to 8:

```
DES-3200-28P:admin#config mac_based_access_control ports 1-8 max_users no_limit
Command: config mac_based_access_control ports 1-8 max_users no_limit

Success.

DES-3200-28P:admin#
```

To configure the MAC-based Access Control timer parameters to have an infinite aging time and a block time of 120 seconds on ports 1 to 8:

```
DES-3200-28P:admin#config mac_based_access_control ports 1-8 aging_time
infinite block_time 120
Command: config mac_based_access_control ports 1-8 aging_time infinite
block_time 120

Success.

DES-3200-28P:admin#
```

40-7 create mac_based_access_control

Description

This command is used to assign a static 802.1Q VLAN as a MAC-based Access Control guest VLAN.

Format

create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

Parameters

guest_vlan - Specify MAC-based Access Control guest VLAN by name, it must be a static 1Q VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
guest_vlanid - Specify MAC-based Access Control guest VLAN by VID, it must be a static 1Q VLAN. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

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

Example

To create a MAC-based Access Control guest VLAN:

```
DES-3200-28P:admin#create mac_based_access_control guest_vlan VLAN8
Command: create mac_based_access_control guest_vlan VLAN8

Success.

DES-3200-28P:admin#
```

40-8 delete mac_based_access_control

Description

This command is used to remove a MAC-based Access Control guest VLAN.

Format

delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

Parameters

guest_vlan - Specify the name of the MAC-based Access Control's guest VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
guest_vlanid - Specify the VID of the MAC-based Access Control's guest VLAN. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

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

Example

To delete the MAC-based Access Control guest VLAN called default:

```
DES-3200-28P:admin#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

DES-3200-28P:admin#
```

40-9 clear mac_based_access_control auth_state

Description

This command is used to clear the authentication state of a user (or port). The port (or the user) will return to an un-authenticated state. All the timers associated with the port (or the user) will be reset.

Format

clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]

Parameters

ports - To specify the port range to delete MAC addresses on them. **all** - To specify all MAC-based Access Control enabled ports to delete MAC addresses. **<portlist>** - Enter the list of port used for this configuration here.
mac_addr - To delete a specified host with this MAC address. **<macaddr>** - Enter the MAC address used here.

Restrictions

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

Example

To clear MAC-based Access Control clients' authentication information for all ports:

```
DES-3200-28P:admin#clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DES-3200-28P:admin#
```

To delete the MAC-based Access Control authentication information for the host that has a MAC address of 00-00-00-47-04-65:

```
DES-3200-28P:admin#clear mac_based_access_control auth_state mac_addr 00-00-00-
47-04-65
Command: clear mac_based_access_control auth_state mac_addr 00-00-00-47-04-65

Success.

DES-3200-28P:admin#
```

40-10 create mac_based_access_control_local

Description

This command is used to create a MAC-based Access Control local database entry that will be used for authentication. This command can also specify the VLAN that an authorized host will be assigned to.

Format

create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid < vlanid 1-4094>]}

Parameters

mac - Specify the MAC address that can pass local authentication. **<macaddr>** - Enter the MAC address used here.
vlan - (Optional) Specify the target VLAN by using the VLAN name. When this host is authorized, it will be assigned to this VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specify the target VLAN by using the VID. When this host is authorized, it will be assigned to this VLAN if the target VLAN exists. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
If no vlanid or vlan parameter is specified, not specify the target VLAN for this host.

Restrictions

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

Example

To create one MAC-based Access Control local database entry for MAC address 00-00-00-00-00-01 and specify that the host will be assigned to the “default” VLAN after the host has been authorized:

```
DES-3200-28P:admin#create mac_based_access_control_local mac 00-00-00-00-00-01
vlan default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default

Success.

DES-3200-28P:admin#
```

40-11 config mac_based_access_control_local

Description

This command is used to configure a MAC-based Access Control local database entry.

Format

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

Parameters

mac - Specify the authenticated host’s MAC address. **<macaddr>** - Enter the MAC address used here.
vlan - Specify the target VLAN by VLAN name. When this host is authorized, the host will be assigned to this VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specify the target VLAN by VID. When this host is authorized, the host will be assigned to this VLAN if the target VLAN exists. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
clear_vlan - Not specify the target VLAN. When this host is authorized, will not assign target VLAN.

Restrictions

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

Example

To configure the target VLAN “default” for the MAC-based Access Control local database entry 00-00-00-00-00-01:

```
DES-3200-28P:admin#config mac_based_access_control_local mac 00-00-00-00-00-01
vlan default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default

Success.

DES-3200-28P:admin#
```

40-12 delete mac_based_access_control_local

Description

This command is used to delete a MAC-based Access Control local database entry.

Format

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

mac - Delete local database entry by specific MAC address. **<macaddr>** - Enter the MAC address used here.
vlan - Delete local database entries by specific target VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Delete local database entries by specific target VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

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

Example

To delete the MAC-based Access Control local database entry for MAC address 00-00-00-00-00-01:

```
DES-3200-28P:admin#delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DES-3200-28P:admin#
```

To delete the MAC-based Access Control local database entry for the VLAN name VLAN3:

```
DES-3200-28P:admin#delete mac_based_access_control_local vlan VLAN3
Command: delete mac_based_access_control_local vlan VLAN3

Success.

DES-3200-28P:admin#
```

40-13 config mac_based_access_control authorization attributes

Description

This command is used to enable or disable the acceptation of an authorized configuration.

When authorization is enabled for MAC-based Access Controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled.

When authorization is enabled for MAC-based Access Controls with local authentication, the authorized attributes assigned by the local database will be accepted.

Format

config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

Parameters

radius - (Optional) If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled. The default state is enabled. **enable** - Specify that the radius attributes will be enabled. **disable** - Specify that the radius attributes will be disabled.
local - (Optional) If specified to enable, the authorized attributes assigned by the local database will be accepted if the global authorization status is enabled. The default state is enabled. **enable** - Specify that the local attributes will be enabled. **disable** - Specify that the local attributes will be disabled.

Restrictions

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

Example

The following example will disable the configuration authorized from the local database:

```
DES-3200-28P:admin#config mac_based_access_control authorization attributes
local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

DES-3200-28P:admin#
```

40-14 show mac_based_access_control

Description

This command is used to display the MAC-based Access Control setting.

Format

show mac_based_access_control {ports {<portlist>}}

Parameters

ports – (Optional) Displays the MAC-based Access Control settings for a specific port or range of ports. **<portlist>** - (Optional) Enter the list of port used for this configuration here.
If no parameter is specified, the global MAC-based Access Control settings will be displayed.

Restrictions

None.

Example

To show the MAC-based Access Control port configuration for ports 1 to 4:

```
DES-3200-28P:admin#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4


Port    State     Aging Time   Block Time  Auth Mode    Max User
                    (min)        (sec)
-----  --------   ----------   ---------   ----------   --------
1      Disabled   1440         300         Host-based   128
2      Disabled   1440         300         Host-based   128
3      Disabled   1440         300         Host-based   128
4      Disabled   1440         300         Host-based   128

DES-3200-28P:admin#
```

40-15 show mac_based_access_control_local

Description

This command is used to display the MAC-based Access Control local database entry(s).

Format

show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac - (Optional) Displays MAC-based Access Control local database entries for a specific MAC

address. **<macaddr>** - Enter the MAC address used here.
vlan - (Optional) Displays MAC-based Access Control local database entries for a specific target VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Displays MAC-based Access Control local database entries for a specific target VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
If the parameter is no specified, displays all MAC-based Access Control local database entries.

Restrictions

None.

Example

To show MAC-based Access Control local database for the VLAN called 'default':

```
DES-3200-28P:admin#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address         VID
-----------------  ----
00-00-00-00-00-01  1
00-00-00-00-00-04  1

Total Entries:2

DES-3200-28P:admin#
```

40-16 show mac_based_access_control auth_state

Description

This command is used to display the MAC-based Access Control authentication status.

Format

show mac_based_access_control auth_state ports {<portlist>}

Parameters

ports - Display authentication status by specific port. **<portlist>** - (Optional) Enter the list of port used for this configuration here.
If not specified port(s), it will display all of MAC-based Access Control ports authentication status.

Restrictions

None.

Example

To display the MAC-based Access Control authentication status on port 1-4

```
DES-3200-28P:admin#show mac_based_access_control auth_state ports 1-4
Command: show mac_based_access_control auth_state ports 1-4


 (P): Port-based

Port MAC Address          State          VID  Priority Aging Time/
                                                       Block Time
---- -------------------- -------------- ---- -------- ------------

Total Authenticating Hosts  : 0
Total Authenticated Hosts   : 0
Total Blocked Hosts         : 0


DES-3200-28P:admin#
```

40-17 config mac_based_access_control max_users

Description

This command is used to configure the maximum number of authorized clients.

Format

config mac_based_access_control max_users [<value 1-1000> | no_limit]

Parameters

max_users - Specify to set the maximum number of authorized clients on the whole device.
<value 1-1000> - Enter the maximum users here. This value must be between 1 and 1000.
no_limit - Specify to not limit the maximum number of users on the system. By default, there is no limit on the number of users.

Restrictions

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

Example

To configure the maximum number of users of the MAC-based Access Control system supports to 128:

```
DES-3200-28P:admin#config mac_based_access_control max_users 128
Command: config mac_based_access_control max_users 128

Success.

DES-3200-28P:admin#
```

40-18 config mac_based_access_control trap state

Description

This command is used to enable or disable sending of MAC-based Access Control traps.

Format

config mac_based_access_control trap state [enable | disable]

Parameters

enable - Enable trap for MAC-based Access Control. The trap of MAC-based Access Control will be sent out.
disable - Disable trap for MAC-based Access Control.

Restrictions

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

Example

To enable trap state of MAC-based Access Control:

```
DES-3200-28P:admin#config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

DES-3200-28P:admin#
```

40-19 config mac_based_access_control log state

Description

This command is used to enable or disable generating of MAC-based Access Control logs.

Format

config mac_based_access_control log state [enable | disable]

Parameters

enable - Enable log for MAC-based Access Control. The log of MAC-based Access Control will be generated.
disable - Disable log for MAC-based Access Control.

Restrictions

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

Example

To disable log state of MAC-based Access Control:

```
DES-3200-28P:admin#config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

DES-3200-28P:admin#
```

Chapter 41 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>]}

41-1 create mac_based_vlan mac_address

Description

This command is used to create a static MAC-based VLAN entry.

This command only needs to be supported by the model which supports MAC-based VLAN.

There is a global limitation of the maximum entries supported for the static MAC-based entry.

Format

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

mac_address - Specify the MAC address used. **<macaddr>** - Enter the MAC address here.
vlan - The VLAN to be associated with the MAC address. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specify the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

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

Example

To create a static MAC-based VLAN entry:

```
DES-3200-28P:admin#create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid
100
Command: create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100

Success.

DES-3200-28P:admin#
```

41-2 delete mac_based_vlan

Description

This command is used to delete the static MAC-based VLAN entry.

Format

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specify the MAC address used. **<macaddr>** - Enter the MAC address used here.
vlan - (Optional) The VLAN to be associated with the MAC address. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specify the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
If no parameter is specified, ALL static configured entries will be removed.

Restrictions

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

Example

To delete a static MAC-based VLAN entry:

```
DES-3200-28P:admin#delete mac_based_vlan mac_address 00-11-22-33-44-55 vlanid
100
Command: delete mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100

Success.

DES-3200-28P:admin#
```

41-3 show mac_based_vlan

Description

This command is used to display the static or dynamic MAC-Based VLAN entry. If the MAC address and VLAN is not specified, all static and dynamic entries will be displayed.

Format

show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specify the entry that you would like to display. **<macaddr>** - Enter the MAC address used here.

vlan - (Optional) Specify the VLAN that you would like to display. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specify the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

None.

Example

In the following example, MAC address “00-80-c2-33-c3-45” is assigned to VLAN 300 by manual config. It is assigned to VLAN 400 by Voice VLAN. Since Voice VLAN has higher priority than manual configuration, the manual configured entry will become inactive. To display the MAC-based VLAN entry:

```
DES-3200-28P:admin#show mac_based_vlan

    MAC Address       VLAN ID        Status        Type
----------------     -------        --------      -------------------
00-80-e0-14-a7-57     200            Active        Static
00-80-c2-33-c3-45     300            Inactive      Static
00-80-c2-33-c3-45     400            Active        Voice VLAN

Total Entries : 3

DES-3200-28P:admin#
```

Chapter 42 Mirror Command List

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

42-1 config mirror

Description

This command is used to configure a mirror port − source port pair on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe then can be attached to study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, please note that the target port must be configured in the same VLAN and operates at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.

Format

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

Parameters

port - The port that will receive the packets duplicated at the mirror port. **<port>** - Enter the port number to be configured here.
add - (Optional) The mirror entry to be added.
delete - (Optional) The mirror entry to be deleted.
source ports - (Optional) The port that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port. **<portlist>** - Enter the list of port to be configured here.
rx - (Optional) Allows the mirroring packets received (flowing into) the port or ports in the port list.
tx - (Optional) Allows the mirroring packets sent (flowing out of) the port or ports in the port list.
both - (Optional) Mirrors all the packets received or sent by the port or ports in the port list.

Restrictions

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

Example

To add the mirroring ports:

```
DES-3200-28P:admin#config mirror port 3 add source ports 7-12 both
Command: config mirror port 3 add source ports 7-12 both

Success.

DES-3200-28P:admin#
```

42-2 enable mirror

Description

This command is used to enable mirror function without having to modify the mirror session configuration.

Format

enable mirror

Parameters

None.

Restrictions

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

Example

To enable mirroring function:

```
DES-3200-28P:admin#enable mirror
Command: enable mirror

Success.

DES-3200-28P:admin#
```

42-3 disable mirror

Description

This command is used to disable mirror function without having to modify the mirror session configuration.

Format

disable mirror

Parameters

None.

Restrictions

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

Example

To disable mirroring function:

```
DES-3200-28P:admin#disable mirror
Command: disable mirror

Success.

DES-3200-28P:admin#
```

42-4 show mirror

Description

This command is used to display the current mirror function state and mirror session configuration on the Switch.

Format

show mirror

Parameters

None.

Restrictions

None.

Example

To display mirroring configuration:

```
DES-3200-28P:admin#show mirror
Command: show mirror

Current Settings
Mirror Status: Enabled
Target Port  : 3
Mirrored Port
           RX: 7-12
           TX: 7-12

DES-3200-28P:admin#
```

Chapter 43 MSTP debug enhancement Command List

debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]
debug stp show information
debug stp show flag {ports <portlist>}
debug stp show counter {ports [<portlist> | all]}
debug stp clear counter {ports[<portlist> | all]}
debug stp state [enable | disable]

43-1 debug stp config ports

Description

This command is used to configure per-port STP debug level on the specified ports.

Format

debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]

Parameters

<portlist> - Specify the STP port range to debug.
all - Specify to debug all ports on the Switch.
event - Debug the external operation and event processing.
bpdu - Debug the BPDU's that have been received and transmitted.
state_machine - Debug the state change of the STP state machine.
all - Debug all of the above.
state - Specify the state of the debug mechanism. **disable** - Disables the debug mechanism. **brief** - Sets the debug level to brief. **detail** - Sets the debug level to detail.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure all STP debug flags to brief level on all ports:

```
DES-3200-28P:admin#debug stp config ports all all state brief
Command: debug stp config ports all all state brief

Success.

DES-3200-28P:admin#
```

43-2 debug stp show information

Description

This command is used to display STP detailed information, such as the hardware tables, the STP state machine, etc.

Format

debug stp show information

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show STP debug information:

```
DES-3200-28P:admin#debug stp show information
Command: debug stp show information

Warning: only support local device.
Spanning Tree Debug Information:
---------------------------------------
Port Status In Hardware Table:
Instance 0:
Port 1   : FOR  Port 2   : FOR  Port 3   : FOR  Port 4   : FOR  Port 5   : FOR
Port 6   : FOR
Port 7   : FOR  Port 8   : FOR  Port 9   : FOR  Port 10  : FOR  Port 11  : FOR
Port 12  : FOR
Port 13  : FOR  Port 14  : FOR  Port 15  : FOR  Port 16  : FOR  Port 17  : FOR
Port 18  : FOR
Port 19  : FOR  Port 20  : FOR  Port 21  : FOR  Port 22  : FOR  Port 23  : FOR
Port 24  : FOR
Port 25  : FOR  Port 26  : FOR  Port 27  : FOR  Port 28  : FOR
-------------------------------------
Root Priority And Times:
Instance 0:
 Designated Root Bridge : 29683/DD-FE-F7-F8-DF-DA
 External Root Cost     : -336244805
 Regional Root Bridge   : 57055/6F-D1-FD-2F-08-B7
 Internal Root Cost     : -107020353
 Designated Bridge      : 57851/FD-EF-EF-C9-FC-9B
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

43-3 debug stp show flag

Description

This command is used to display the STP debug level on specified ports.

Format

debug stp show flag {ports <portlist>}

Parameters

ports - (Optional) Specify the STP ports to display. **<portlist>** - (Optional) Enter the list of port used for this configuration here.
If no parameter is specified, all ports on the Switch will be displayed.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the debug STP levels on all ports:

```
DES-3200-28P:admin#debug stp show flag
DES-3200-28P:admin#debug stp show flag
Command: debug stp show flag

Global State: Disabled

Port Index       Event Flag       BPDU Flag       State Machine Flag
-------------------------------------------------------------
 1               Disabled         Disabled        Disabled
 2               Disabled         Disabled        Disabled
 3               Disabled         Disabled        Disabled
 4               Disabled         Disabled        Disabled
 5               Disabled         Disabled        Disabled
 5               Disabled         Disabled        Disabled
 7               Disabled         Disabled        Disabled
 8               Disabled         Disabled        Disabled
 9               Disabled         Disabled        Disabled
 10              Disabled         Disabled        Disabled
 11              Disabled         Disabled        Disabled
 12              Disabled         Disabled        Disabled
 13              Disabled         Disabled        Disabled
 14              Disabled         Disabled        Disabled
 15              Disabled         Disabled        Disabled
 16              Disabled         Disabled        Disabled
 17              Disabled         Disabled        Disabled
 18              Disabled         Disabled        Disabled
 19              Disabled         Disabled        Disabled
 20              Disabled         Disabled        Disabled
 21              Disabled         Disabled        Disabled
```

```
 22              Disabled         Disabled        Disabled
 23              Disabled         Disabled        Disabled
 24              Disabled         Disabled        Disabled
 25              Disabled         Disabled        Disabled
 26              Disabled         Disabled        Disabled
 27              Disabled         Disabled        Disabled
 28              Disabled         Disabled        Disabled

DES-3200-28P:admin#
```

43-4 debug stp show counter

Description

This command is used to display the STP counters.

Format

debug stp show counter {ports [<portlist> | all]}

Parameters

ports - (Optional) Specify the STP ports for display. **<portlist>** - Enter the list of port used for this configuration here. **all** - Display all port's counters.
If no parameter is specified, display the global counters.

Restrictions

Only Administrator-level users can issue this command.

Example

To show the STP counters for port 9:

```
DES-3200-28P:admin#debug stp show counter ports 9
Command: debug stp show counter ports 9

STP Counters
-------------------------------------
 Port 9    :
  Receive:                                  Transmit:
  Total STP Packets         : 0             Total STP Packets  : 0
  Configuration BPDU        : 0             Configuration BPDU : 0
  TCN BPDU                  : 0             TCN BPDU           : 0
  RSTP TC-Flag              : 0             RSTP TC-Flag       : 0
  RST BPDU                  : 0             RST BPDU           : 0

  Discard:
  Total Discarded BPDU      : 0
  Global STP Disabled       : 0
  Port STP Disabled         : 0
  Invalid packet Format     : 0
  Invalid Protocol          : 0
  Configuration BPDU Length : 0
  TCN BPDU Length           : 0
  RST BPDU Length           : 0
  Invalid Type              : 0
  Invalid Timers            : 0

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

43-5 debug stp clear counter

Description

This command is used to clear the STP counters.

Format

debug stp clear counter {ports[<portlist> | all]}

Parameters

ports – (Optional)Specify the port range.
<portlist> - Enter the list of port used for this configuration here.
all - Clears all port counters.

Restrictions

Only Administrator-level users can issue this command.

Example

To clear all STP counters on the Switch:

```
DES-3200-28P:admin#debug stp clear counter ports all
Command: debug stp clear counter ports all

Success.

DES-3200-28P:admin#
```

43-6 debug stp state

Description

This command is used to enable or disable the STP debug state.

Format

debug stp state [enable | disable]

Parameters

state - Specify the STP debug state. **enable** - Enable the STP debug state. **disable** - Disable the STP debug state.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the STP debug state to enable, and then disable the STP debug state:

```
DES-3200-28P:admin#debug stp state enable
Command: debug stp state enable

Success.

DES-3200-28P:admin#debug stp state disable
Command: debug stp state disable

Success.

DES-3200-28P:admin#
```

Chapter 44 Multicast Filter Command List

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-24> profile_name <name 1-32>
config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcast_address_list>}(1)
config mcast_filter_profile ipv6 [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)
delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-24> | all] | profile_name <name 1-32>]
show mcast_filter_profile {[ipv4 | ipv6]} {[profile_id <value 1-24> | profile_name <name 1-32>]}
config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} { [add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] | access [permit | deny]}
config max_mcast_group [ports <portlist> | vlanid <vlanid_list] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]}(1)
show max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
show limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
config cpu_filter l3_control_pkt <portlist> [{dvmrp|pim|igmp_query |ospf | rip | vrrp} | all] state [enable | disable]
show cpu_filter l3_control_pkt ports {<portlist>}

44-1 create mcast_filter_profile

Description

This command is used to configure a multicast address profile. Multiple ranges of multicast addresses can be defined in the profile. If the IPv4 or ipv6 option is not specified, IPv4 is implied.

Format

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-24> profile_name <name 1-32>

Parameters

ipv4 - (Optional) Adds an IPv4 multicast profile. **ipv6** - (Optional) Adds an IPv6 multicast profile.
profile_id - The ID of the profile. Range is 1 to n. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - Provides a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.

Restrictions

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

Example

To create a multicast address profile with a profile ID of 2 and a profile name of MOD:

```
DES-3200-28P:admin#create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

DES-3200-28P:admin#
```

44-2 config mcast_filter_profile

Description

This command is used to add or delete a range of multicast IP addresses to or from the profile.

Format

config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcast_address_list>}(1)

Parameters

profile_id - ID of the profile. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - Provides a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. THe profile name can be up to 32 characters long.
profile_name - (Optional) Provides a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
add - (Optional) Specify to add a multicast address.
delete - (Optional) Specify to delete a multicast address.
<mcast_address_list> - (Optional) List of the multicast addresses to be put in the profile. You can either specify a single multicast IP address or a range of multicast addresses using -.

Restrictions

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

Example

To add the multicast address range 225.1.1.1 to 225.1.1.10 to the profile:

```
DES-3200-28P:admin#config mcast_filter_profile profile_id 2 add 225.1.1.1 -
225.1.1.10
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.10

Success.

DES-3200-28P:admin#
```

44-3 config mcast_filter_profile ipv6

Description

This command is used to add or delete a range of IPv6 multicast addresses to the profile.

Format

config mcast_filter_profile ipv6 [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)

Parameters

profile_id - ID of the profile. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - Provides a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
profile_name - (Optional) Provides a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
add - (Optional) Specify to add an IPv6 multicast address.
delete - (Optional) Specify to delete an IPv6 multicast address.
<mcastv6_address_list> - (Optional) Lists the IPv6 multicast addresses to put in the profile. You can either specify a single IPv6 multicast IP address or a range of IPv6 multicast addresses connected by '-'.

Restrictions

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

Example

To add the IPv6 multicast address range FFF0E::100:0:0:20 – FFF0E::100:0:0:22 to profile ID 3:

```
DES-3200-28P:admin#config mcast_filter_profile ipv6 profile_id 3 add
FF0E::100:0:0:20– FFF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20–
FFF0E::100:0:0:22

Success.

DES-3200-28P:admin#
```

44-4 delete mcast_filter_profile

Description

This command is used to delete a multicast address profile. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-24> | all] | profile_name <name 1-32>]

Parameters

ipv4 - (Optional) Specify to delete an IPv4 multicast profile.
ipv6 - (Optional) Specify to delete an IPv6 multicast profile.
profile_id - Specify the ID of the profile

<value 1-24> - Enter the profile ID value here. This value must be between 1 and 24. **all** - All multicast address profiles will be deleted.
profile_name - Specify to display a profile based on the profile name. **<name 1-32>** - Enter the profile name value here. The profile name can be up to 32 characters long.

Restrictions

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

Example

To delete the multicast address profile with a profile ID of 3:

```
DES-3200-28P:admin#delete mcast_filter_profile profile_id  3
Command: delete mcast_filter_profile profile_id  3
Success.

DES-3200-28P:admin#
```

To delete the multicast address profile called MOD:

```
DES-3200-28P:admin#delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Total entries: 2

DES-3200-28P:admin#
```

44-5 show mcast_filter_profile

Description

This command is used to display the defined multicast address profiles. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show mcast_filter_profile {[ipv4 | ipv6]} {[profile_id <value 1-24> | profile_name <name 1-32>]}

Parameters

ipv4 - (Optional) Specify to delete an IPv4 multicast profile.
ipv6 - (Optional) Specify to delete an IPv6 multicast profile.
profile_id - (Optional) Specify the ID of the profile **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - (Optional) Specify to display a profile based on the profile name. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.

Restrictions

None.

Example

To display all the defined multicast address profiles:

```
DES-3200-28P:admin#show mcast_filter_profile
Command: show mcast_filter_profile

Profile ID       Name        Multicast Addresses
----  ----------------  ----------------  ----------------
1                MOD        234.1.1.1 - 238.244.244.244
                            234.1.1.1 - 238.244.244.244
2              customer     224.19.62.34 - 224.19.162.200

Total Entries : 2

DES-3200-28P:admin#
```

44-6 config limited_multicast_addr

Description

This command is used to configure the multicast address filtering function on a port or VLAN. When there are no profiles specified with a port or VLAN, the limited function is not effective. When the function is configured on a port, it limits the multicast group operated by the IGMP or MLD snooping function. When this function is configured on a VLAN, the multicast group is limited to only operate the IGMP or MLD layer 3 functions. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {[add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] | access [permit | deny]}

Parameters

ports - Specify the range of ports to configure the multicast address filtering function. **<portslist>** - Enter the list of port to be configured here.
vlanid - Specify the VLAN ID of the VLAN that the multicast address filtering function will be configured on. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specify the IPv4 multicast profile.
ipv6 - (Optional) Specify the IPv6 multicast profile.
add - (Optional) Adds a multicast address profile to a port.
delete - (Optional) Delete a multicast address profile to a port.
profile_id - (Optional) A profile to be added to or deleted from the port. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - (Optional) Specify the profile name used. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
access - (Optional) Specify the access of packets matching the addresses defined in the profiles. **permit** - Specify that packets matching the addresses defined in the profiles will be permitted. The default mode is permit. **deny** - Specify that packets matching the addresses defined in the profiles will be denied.

Restrictions

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

Example

To add multicast address profile 2 to ports 1 and 3:

```
DES-3200-28P:admin#config limited_multicast_addr ports 1,3  add profile_id 2
Command: config limited_multicast_addr ports 1,3  add profile_id 2

Success.

DES-3200-28P:admin#
```

44-7 config max_mcast_group

Description

This command is used to configure the maximum number of multicast groups that a port can join.

If the IPv4 or IPv6 option is not specified, IPv4 is implied.

When the joined groups for a port or a VLAN have reached the maximum number, the newly learned group will be dropped if the action is specified as drop. The newly learned group will replace the eldest group if the action is specified as replace.

Format

config max_mcast_group [ports <portlist> | vlanid <vlanid_list] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]}(1)

Parameters

ports - Specify the range of ports to configure the max_mcast_group. **<portlist>** - Enter the list of ports to be configured here.
vlanid - Specify the VLAN ID to configure max_mcast_group. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specify that the maximum number of IPv4 learned addresses should be limited.
ipv6 - (Optional) Specify that the maximum number of IPv6 learned addresses should be limited.
max_group - (Optional) Specify the maximum number of multicast groups. The range is from 1 to n or infinite. “Infinite” means that the maximum number of multicast groups per port or VLAN is not limited by the Switch. **<value 1-1024>** - Enter the maximum group value here. This value must be between 1 and 1024. **infinite** - Specify that the maximum group value will be set to infinite.
action - (Optional) Specify the action for handling newly learned groups when the register is full. **drop** - The new group will be dropped. **replace** - The new group will replace the eldest group in the register table.

Restrictions

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

Example

To configure the maximum number of multicast group that ports 1 and 3 can join to 100:

```
DES-3200-28P:admin#config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DES-3200-28P:admin#
```

44-8 show max_mcast_group

Description

This command is used to display the maximum number of multicast groups that a port can join. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}

Parameters

ports - Specify the range of ports for displaying information about the maximum number of multicast groups that the specified ports can join. **<portlist>** - Enter the list of ports to be configured here.
vlanid - Specify the VLAN ID for displaying the maximum number of multicast groups. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specify to display the maximum number of IPv4 learned addresses.
ipv6 - (Optional) Specify to display the maximum number of IPv6 learned addresses.

Restrictions

None.

Example

To display the maximum number of multicast groups that ports 1 and 2 can join:

```
DES-3200-28P:admin#show max_mcast_group ports 1-2
Command: show max_mcast_group ports 1-2

Port      Max Multicast Group Number    Action
------    --------------------------  ---------
1         100                           Drop
2         Infinite                      Drop

Total Entries: 2


DES-3200-28P:admin#
```

To display the maximum number of multicast groups that VLANs 1 and 2 can join:

```
DES-3200-28P:admin#show max_mcast_group vlanid 1-2
Command: show max_mcast_group vlanid 1-2

VLAN      Max Multicast Group Number    Action
------    --------------------------  ---------
1         Infinite                      Drop
2         10                            Drop

Total Entries: 2

DES-3200-28P:admin#
```

44-9 show limited_multicast_addr

Description

This command is used to display the multicast address range by port or by VLAN.

When the function is configured on a port, it limits the multicast groups operated by the IGMP or MLD snooping function and layer 3 functions. When the function is configured on a VLAN, it limits the multicast groups operated by the IGMP or MLD layer 3 functions.

If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}

Parameters

ports - Specify the range of ports that require information displaying about the multicast address filtering function. **<portlist>** - Enter the list of port to be configured here.
vlanid - Specify the VLAN ID of VLANs that require information displaying about the multicast address filtering function. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specify to display the IPv4 multicast profile associated with the port.
ipv6 - (Optional) Specify to display the IPv6 multicast profile associated with the port.

Restrictions

None.

Example

To show the limited multicast address range on ports 1 and 3:

```
DES-3200-28P:admin#show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Port    : 1
Access  : Deny

Profile ID      Name                Multicast Addresses
-----------    -----------        ----------------------------
1              customer             224.19.62.34 - 224.19.162.200

Port    : 3
Access  : Deny

Profile ID      Name                Multicast Addresses
-----------    ---------------   ----------------------------
1              customer          224.19.62.34 - 224.19.162.200

DES-3200-28P:admin#
```

To show the limited multicast settings configured on VLAN 1:

```
DES-3200-28P:admin#show limited_multicast_addr vlan 1
Command: show limited_multicast_addr vlan 1

VLAN ID     : 1
Access      : Deny

Profile ID      Name               Multicast Addresses
----------  -----------------    ----------------------------
1           customer               224.19.62.34 - 224.19.162.200


Success.

DES-3200-28P:admin#
```

44-10 config cpu_filter l3_control_pkt

Description

This command is used to configure the port state for the Layer 3 control packet filter.

Format

config cpu_filter l3_control_pkt <portlist> [{dvmrp|pim|igmp_query |ospf | rip | vrrp} | all] state [enable | disable]

Parameters

<portlist> - Specify the port list to filter control packets. **dvmrp** – (Optional) Specify to filter the DVMRP control packets. **pim** - (Optional) Specify to filter the PIM control packets.

igmp_query - (Optional) Specify to filter the IGMP query control packets. **ospf -** (Optional) Specify to filter the OSPF control packets. **rip -** (Optional) Specify to filter the RIP control packets. **vrrp -** (Optional) Specify to filter the VRRP control packets. **all** - Specify to filter all the L3 protocol control packets.
state - Specify the filter function status. The default is disabled. **enable** - Enable the filtering function. **disable** - Disable the filtering function.

Restrictions

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

Example

To filter the DVMRP control packets on ports 1 to 2:

```
DES-3200-28P:admin#config cpu_filter l3_control_pkt 1-2 dvmrp state enable
Command: config cpu_filter l3_control_pkt 1-2 dvmrp state enable

Success.

DES-3200-28P:admin#
```

44-11 show cpu_filter l3_control_pkt ports

Description

This command is used to display the L3 control packet CPU filtering state.

Format

show cpu_filter l3_control_pkt ports {<portlist>}

Parameters

<portlist> - (Optional) Specify the port list to display the L3 control packet CPU filtering state.

Restrictions

None.

Example

To display the filtering status for port 1 and 2:

```
DES-3200-28P:admin#show cpu_filter l3_control_pkt ports 1-2
Command: show cpu_filter l3_control_pkt ports 1-2

 Port    IGMP Query    DVMRP         PIM        OSPF         RIP       VRRP
 ----   ----------    --------    --------    --------    --------    --------
 1       Disabled      Enabled      Disabled      Disabled    Disabled    Disabl
ed
 2       Disabled      Enabled      Disabled      Disabled    Disabled    Disabl
ed

DES-3200-28P:admin#
```

Chapter 45 Multicast VLAN Command List

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}
config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable|disable] | replace_source_ip <ipaddr> | remap_priority [<value 0-7> | none] {replace_priority}}
create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>
config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>
delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]
show igmp_snooping multicast_vlan_group_profile {< profile_name 1-32>}
config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>
show igmp_snooping multicast_vlan_group {<vlan_name 32>}
delete igmp_snooping multicast_vlan <vlan_name 32>
enable igmp_snooping multicast_vlan
disable igmp_snooping multicast_vlan
config igmp_snooping multicast_vlan forward_unmatched [enable | disable]
show igmp_snooping multicast_vlan {<vlan_name 32>}

45-1 create igmp_snooping multicast_vlan

Description

This command is used to create a multicast VLAN and implements relevant parameters as specified. More than one multicast VLANs can be configured. The maximum number of configurable VLANs is 5.

Newly created IGMP snooping multicast VLANs must use a unique VLAN ID and name, i.e. they cannot use the VLAN ID or name of any existing 802.1q VLAN.

Also keep in mind the following conditions:

- Multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands.
- An IP interface cannot be bound to a multicast VLAN.
- The multicast VLAN snooping function co-exists with the 802.1q VLAN snooping function.

Format

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

Parameters

<vlan_name 32> - Enter the multicast VLAN here. The VLAN name can be up to 32 characters long.

<vlanid 2-4094> - The VLAN ID of the multicast VLAN to be created. This value must be between 2 and 4094.
remap_priority - (Optional) The remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority will be used. The default setting is none. **<value 0-7>** - Enter the remap priority value here. This value must be between 0 and 7. **none** - Specify that the remap priority value will be set to none.
replace_priority - (Optional) Specify that packet's priority will be changed by the Switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Restrictions

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

Example

To create an IGMP snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DES-3200-28P:admin#create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2

Success.

DES-3200-28P:admin#
```

45-2 config igmp_snooping multicast_vlan

Description

This command is used to add member ports and source ports to a list of multicast VLAN member ports. Member ports automatically become untagged members of the multicast VLAN and source ports automatically become tagged members of the multicast VLAN. However, member ports of one multicast VLAN are allowed to overlap with member ports on a different multicast VLAN.

A multicast VLAN must first be created using the create igmp_snooping multicast_vlan command before the multicast VLAN can be configured.

Format

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable|disable] | replace_source_ip <ipaddr> | remap_priority [<value 0-7> | none] {replace_priority}}

Parameters

<vlan_name 32> - Enter the multicast VLAN here. The VLAN name can be up to 32 characters long.
add - Specify that the port will be added to the specified multicast VLAN.
delete - Specify that the port will be deleted from the specified multicast VLAN.
member_port - A member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN. **<portlist>** - Enter the list of port to be configured here.
source_port - A port or range of ports to be added to the multicast VLAN.

<portlist> - Enter the list of port to be configured here.
untag_source_port - Specify the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN. **<portlist>** - Enter the list of port to be configured here.
tag_member_port - Specify the port or range of ports that will become tagged members of the multicast VLAN. **<portlist>** - Enter the list of port to be configured here.
state - Used to specify if the multicast VLAN for a chosen VLAN should be enabled or disabled. **enable** - Specify to enable the multicast VLAN for a chosen VLAN. **disable** - Specify to disable the multicast VLAN for a chosen VLAN.
replace_source_ip - Before forwarding the report packet sent by the host, the source IP address in the join packet must be replaced by this IP address. If 0.0.0.0 is specified, the source IP address will not be replaced. **<ipaddr>** - Enter the replace source IP address here.
remap_priority - The remap priority value to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority is used. The default setting is none. **<value 0-7>** - Enter the remap priority value here. This value must be between 0 and 7. **none** - Specify that the remap priority value will be set to none. **replace_priority** - (Optional) Specify that the packet priority will be changed to the remap_priority, but only if remap_priority is set.

Restrictions

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

Example

To configure an IGMP snooping multicast VLAN with the name "v1", make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DES-3200-28P:admin#config igmp_snooping multicast_vlan mv1 add member_port 1,3
state enable
Command: config igmp_snooping multicast_vlan mv1 add member_port 1,3 state
enable

Success.

DES-3200-28P:admin#
```

45-3 create igmp_snooping multicast_vlan_group_profile

Description

This command is used to create an IGMP snooping multicast group profile on the Switch.

Format

create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group profile name here. The name can be up

to 32 characters long.

Restrictions

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

Example

To create an IGMP snooping multicast group profile with the name “test”:

```
DES-3200-28P:admin#create igmp_snooping multicast_vlan_group_profile test
Command: create igmp_snooping multicast_vlan_group_profile test

Success.

DES-3200-28P:admin#
```

45-4 config igmp_snooping multicast_vlan_group_profile

Description

This command is used to configure an IGMP snooping multicast group profile on the Switch and add or delete multicast addresses for the profile.

Format

config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

Parameters

multicast_vlan_group_profile - Specify the multicast VLAN profile name. The maximum length is 32 characters. **<profile_name 1-32>** - Enter the multicast VLAN group name here. This name can be up to 32 characters long.
add - Adds a multicast address list to or from this multicast VLAN profile. The <mcast_address_list> can be a continuous single multicast address, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, a multicast address range, such as 225.1.1.1-225.2.2.2, or both of types, such as 225.1.1.1, 225.1.1.18-225.1.1.20.
delete - Deletes a multicast address list to or from this multicast VLAN profile. The <mcast_address_list> can be a 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 types, such as 225.1.1.1, 225.1.1.18-225.1.1.20.
<mcast_address_list> - Enter the multicast VLAN IP address here.

Restrictions

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

Example

To add the single multicast address 225.1.1.1 to the IGMP snooping multicast VLAN profile named “test”:

```
DES-3200-28P:admin#config igmp_snooping multicast_vlan_group_profile test add
225.1.1.1
Command: config igmp_snooping multicast_vlan_group_profile test add 225.1.1.1

Success.

DES-3200-28P:admin#
```

45-5 delete igmp_snooping multicast_vlan_group_profile

Description

This command is used to delete an IGMP snooping multicast group profile on the Switch. Specify a profile name to delete it. Specify all to remove all profiles along with the groups that belong to that profile.

Format

delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

Parameters

profile_name - Specify the multicast VLAN profile name.
- **<profile_name 1-32>** - Enter the multicast VLAN profile name here. This name can be up to 32 characters long.
- **all** - Specify to delete all the multicast VLAN profiles.

Restrictions

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

Example

To delete an IGMP snooping multicast group profile with the name “MOD”:

```
DES-3200-28P:admin#delete igmp_snooping multicast_vlan_group_profile
profile_name MOD
Command: delete igmp_snooping multicast_vlan_group_profile profile_name MOD

Success.

DES-3200-28P:admin#
```

45-6 show igmp_snooping multicast_vlan_group_profile

Description

This command is used to show the IGMP snooping multicast group profiles.

Format

show igmp_snooping multicast_vlan_group_profile {< profile_name 1-32>}

Parameters

<profile_name 1-32> - (Optional) Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

None.

Example

To display all IGMP snooping multicast VLAN profiles:

```
DES-3200-28P:admin#show igmp_snooping multicast_vlan_group_profile
Command: show igmp_snooping multicast_vlan_group_profile

Profile Name              Multicast Addresses
--------------------  -------------------------------
MOD                        234.1.1.1 - 238.244.244.244
                           239.1.1.1 - 239.2.2.2
Customer                   224.19.62.34 - 224.19.162.200

Total Entries : 2


DES-3200-28P:admin#
```

45-7 config igmp_snooping multicast_vlan_group

Description

This command is used to configure the multicast group learned with the specific multicast VLAN. The following two cases can be considered for examples:

Case 1- The multicast group is not configured, multicast VLANs do not have any member ports overlapping and the join packet received by the member port is learned on only the multicast VLAN that this port is a member of.

Case 2-,The join packet is learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet cannot be classified into any multicast VLAN to which this port belongs, then the join packet will be learned on the natural VLAN of the packet.

Note that a profile cannot overlap in different multicast VLANs. Multiple profiles can be added to a multicast VLAN.

Format

config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.
add - Used to associate a profile to a multicast VLAN.
delete - Used to de-associate a profile from a multicast VLAN.
profile_name - Specify the multicast VLAN profile name. **<profile_name 1-32>** - Enter the multicast VLAN profile name here. The name can be up to 32 characters long.

Restrictions

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

Example

To add an IGMP snooping profile to a multicast VLAN group with the name "v1":

```
DES-3200-28P:admin#config igmp_snooping multicast_vlan_group v1 add
profile_name channel_1
Command: config igmp_snooping multicast_vlan_group v1 add profile_name
channel_1
Success.


DES-3200-28P:admin#
```

45-8 show igmp_snooping multicast_vlan_group

Description

This command is used to show an IGMP snooping multicast VLAN group.

Format

show igmp_snooping multicast_vlan_group {<vlan_name 32>}

Parameters

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

Restrictions

None.

Example

To show all IGMP snooping multicast VLAN groups setup on the Switch:

```
DES-3200-28P:admin#show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group


VLAN Name                       VLAN ID        Multicast Group Profiles
------------------------------  -------  --------------------------------
mv1                             2         test


DES-3200-28P:admin#
```

45-9 delete igmp_snooping multicast_vlan

Description

This command is used to delete an IGMP snooping multicast VLAN.

Format

delete igmp_snooping multicast_vlan <vlan_name 32>

Parameters

multicast_vlan - The name of the multicast VLAN to be deleted. **<vlan_name 32>** -Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

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

Example

To delete an IGMP snooping multicast VLAN called “v1”:

```
DES-3200-28P:admin#delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicat_vlan v1

Success.

DES-3200-28P:admin#
```

45-10 enable igmp_snooping multicast_vlan

Description

This command is used to control the status of the multicast VLAN function.

Format

enable igmp_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the IGMP snooping multicast VLAN function globally:

```
DES-3200-28P:admin#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DES-3200-28P:admin#
```

45-11 disable igmp_snooping multicast_vlan

Description

This command is used to disable the IGMP multicast VLAN function. The command disable igmp_snooping is used to disable the ordinary IGMP snooping function. By default, the multicast VLAN is disabled.

Format

disable igmp_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the IGMP snooping multicast VLAN function:

```
DES-3200-28P:admin#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DES-3200-28P:admin#
```

45-12 config igmp_snooping multicast_vlan forward_unmatched

Description

This command is used to configure the forwarding mode for multicast VLAN unmatched packets. When the Switch receives an IGMP snooping packet, it will match the packet against the multicast profile to determine which multicast VLAN to associate with. If the packet does not match all profiles, the packet will be forwarded or dropped based on this setting.

By default, the packet will be dropped.

Format

config igmp_snooping multicast_vlan forward_unmatched [enable | disable]

Parameters

enable - The packet will be flooded on the VLAN.
disable - The packet will be dropped.

Restrictions

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

Example

To configure the forwarding mode for multicast VLAN unmatched packets：

```
DES-3200-28P:admin#config igmp_snooping multicast_vlan forward_unmatched enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DES-3200-28P:admin#
```

45-13 show igmp_snooping multicast_vlan

Description

This command is used to display information for IGMP snooping multicast VLANs.

Format

show igmp_snooping multicast_vlan {<vlan_name 32>}

Parameters

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

Restrictions

None.

Example

To display all IGMP snooping multicast VLANs:

```
DES-3200-28P:admin#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

IGMP Multicast VLAN Global State        : Disabled
IGMP Multicast VLAN Forward Unmatched   : Disabled

VLAN Name                               : test
VID                                     : 100

Member(Untagged) Ports                  : 1
Tagged Member Ports                     :
Source Ports                            : 3
Untagged Source Ports                   :
Status                                  : Disabled
Replace Source IP                       : 0.0.0.0
Remap Priority                          : None

Total Entries: 1

DES-3200-28P:admin#
```

Chapter 46 Multiple Spanning Tree Protocol (MSTP) Command List

enable stp
disable stp
config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}
show stp
create stp instance_id <value 1-7>
config stp instance_id <value 1-7> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id <value 1-7>
config stp mst_config_id {revision_level <int 0-65535> | name <string>}
show stp mst_config_id
config stp mst_ports <portlist> instance_id <value 0-7> { internalCost [auto | <value 1-200000000>] | priority <value 0-240>}
config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] |edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}
show stp ports {<portlist>}
config stp priority <value 0-61440> instance_id <value 0-7>
config stp version [mstp | rstp | stp]
show stp instance {<value 0-7>}

46-1 enable stp

Description

This command is used to enable STP globally.

Format

enable stp

Parameters

None.

Restrictions

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

Example

To enable STP:

```
DES-3200-28P:admin#enable stp
Command: enable stp

Success.

DES-3200-28P:admin#
```

46-2 disable stp

Description

This command is used to disable STP globally.

Format

disable stp

Parameters

None.

Restrictions

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

Example

To disable STP:

```
DES-3200-28P:admin#disable stp
Command: disable stp

Success.

DES-3200-28P:admin#
```

46-3 config stp

Description

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

Format

config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}

Parameters

maxage - (Optional) Used to determine if a BPDU is valid. The default value is 20.

<value 6-40> - Enter the maximum age value here. This value must be between 6-40.
maxhops - (Optional) Used to restrict the forwarded times of one BPDU. The default value is 20. **<value 6-40>** - Enter the maximum hops value here. This value must be between 6 and 40.
hello_time - (Optional) The time interval for sending configuration BPDUs by the Root Bridge. The default value is 2 seconds. This parameter is for STP and RSTP version. MSTP version uses per-port hellotime parameter. **<value 1-2>** - Enter the hello time value here. This value must be between 1 and 2.
forwarddelay - (Optional) The maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15. **<value 4-30>** - Enter the maximum delay time here. This value must be between 4 and 30.
txholdcount - (Optional) Used to restrict the numbers of BPDU transmitted in a time interval. **<value 1-10>** - Enter the transmitted BPDU restriction value here. This value must be between 1 and 10.
fbpdu - (Optional) To decide if the bridge will flood STP BPDU when STP functionality is disabled. **enable** - Specify that the bridge will flood STP BPDU when STP functionality is disabled **disable** - Specify that the bridge will not flood STP BPDU when STP functionality is disabled
nni_bpdu_addr - (Optional) Used to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or an user defined mutilcast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF. **dot1d** - Specify that the NNI BPDU protocol address value will be set to Dot1d. **dot1ad** - Specify that the NNI BPDU protocol address value will be set to Dot1ad.

Restrictions

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

Example

To configure STP:

```
DES-3200-28P:admin#config stp maxage 25
Command: config stp maxage 25

Success.

DES-3200-28P:admin#
```

46-4 show stp

Description

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

Format

show stp

Parameters

None.

Restrictions

None.

Example

To show STP:

```
DES-3200-28P:admin#show stp
Command: show stp

 STP Bridge Global Settings
 --------------------------
 STP Status          : Enabled
 STP Version         : RSTP
 Max Age             : 25
 Hello Time          : 2
 Forward Delay       : 15
 Max Hops            : 20
 TX Hold Count       : 6
 Forwarding BPDU     : Disabled
 NNI BPDU Address    : dot1d


DES-3200-28P:admin#
```

46-5 create stp instance_id

Description

This command is used to create an MST Instance without mapping the corresponding VLANs.

Format

create stp instance_id <value 1-7>

Parameters

instance_id - Specify the MSTP instance ID. Instance 0 represents for default instance, CIST. **<value 1-7>** - Enter the MSTP instance ID here. This value must be between 1 and 7.

Restrictions

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

Example

To create MSTP instance:

```
DES-3200-28P:admin#create stp instance_id 2
Command: create stp instance_id 2

Success.

DES-3200-28P:admin#
```

46-6 config stp instance_id

Description

This command is used to map or remove the VLAN range of the specified MST instance for the existed MST instances.

Format

config stp instance_id <value 1-7> [add_vlan | remove_vlan] <vidlist>

Parameters

instance_id - Specify the MSTP instance ID. Instance 0 represents for default instance, CIST. **<value 1-7>** - Enter the MSTP instance ID here. This value must be between 1 and 7.
add_vlan - Specify to map the specified VLAN list to an existing MST instance.
remove_vlan - Specify to delete the specified VLAN list from an existing MST instance.
<vidlist> - Specify a list of VLANs by VLAN ID.

Restrictions

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

Example

To map a VLAN ID to an MSTP instance:

```
DES-3200-28P:admin#config stp instance_id 2 add_vlan 1-3
Command: config stp instance_id 2 add_vlan 1-3

Success.

DES-3200-28P:admin#
```

To remove a VLAN ID from an MSTP instance:

```
DES-3200-28P:admin#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DES-3200-28P:admin#
```

46-7 delete stp instance_id

Description

This command is used to delete an MST Instance.

Format

delete stp instance_id <value 1-7>

Parameters

instance_id - Specify the MSTP instance ID. Instance 0 represents for default instance, CIST. **<value 1-7>** - Enter the MSTP instance ID here. This value must be between 1 and 7.

Restrictions

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

Example

To delete an MSTP instance:

```
DES-3200-28P:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DES-3200-28P:admin#
```

46-8 config stp mst_config_id

Description

This command is used to change the name or the revision level of the MST configuration identification.

Format

config stp mst_config_id {revision_level <int 0-65535> | name <string>}

Parameters

name - (Optional) Specify the name given for a specific MST region. **<string>** - Enter the MST region name here.
revision_level - (Optional) The same given name with different revision level also represents different MST regions. **<int 0-65535>** - Enter the revision level here. This value must be between 0 and 65535.

Restrictions

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

Example

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

```
DES-3200-28P:admin#config stp mst_config_id name R&D_BlockG revision_level 1
Commands: config stp mst_config_id name R&D_BlockG revision_level 1

Success.

DES-3200-28P:admin#
```

46-9 show stp mst_config_id

Description

This command is used to show the MST configuration identification.

Format

show stp mst_config_id

Parameters

None.

Restrictions

None.

Example

show STP MST configuration ID:

```
DES-3200-28P:admin#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
---------------------------------------

Configuration Name : 00-22-22-22-22-00                    Revision Level :0
MSTI ID     Vid list
-------     -----------
   CIST     1-4094

DES-3200-28P:admin#
```

46-10 config stp mst_ports

Description

This command is used to configure the ports management parameters.

Format

config stp mst_ports <portlist> instance_id <value 0-7> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}

Parameters

mst_ports - Specify to be distinguished from the parameters of ports only at CIST level. **<portlist>** - Enter a list of ports used for the configuration here.
instance_id - Specify the instance ID used. **<value 0-7>** - Enter the instance ID used here. This value must be between 0 and 7.
internalCost - (Optional) Specify the port path cost used in MSTP. **auto** - Specify that the internal cost value will be set to auto. **<value 1-200000000>** - Enter the internal cost value here. This value must be between 1 and 200000000.
priority - (Optional) Specify the port priority value. **<value 0-240>** - Enter the port priority value here. This value must be between 0 and 240.

Restrictions

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

Example

To configure STP MST ports:

```
DES-3200-28P:admin#config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

DES-3200-28P:admin#
```

46-11 config stp ports

Description

This command is used to configure all the parameters of ports, except for Internal Path Cost and Port Priority.

Format

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable]| restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}

Parameters

<portlist> - Enter a list of ports used for the configuration here.
external_cost - (Optional) The path cost between MST regions from the transmitting Bridge to the CIST Root Bridge. It is only used at CIST level. **auto** - Specify that the external cost value will be set to automatic. **<value 1-200000000>** - Enter the external cost value here. This value must be between 1 and 200000000.

hellotime - (Optional) The default value is 2 . This parameter is for MSTP version. For STP and RSTP version, uses the per system hellotime parameter. **<value 1-2>** - Enter the hello time value here. This value must be between 1 and 2.
migrate - (Optional) Operation of management in order to specify the port to send MSTP BPDU for a delay time. **yes** - Specify that the MSTP BPDU for a delay time will be sent. **no** - Specify that the MSTP BPDU for a delay time will not be sent.
edge - (Optional) To decide if this port is connected to a LAN or a Bridged LAN. **true** - Specify that the specified port(s) is edge. **false** - Specify that the specified port(s) is not edge. **auto** - In auto mode, the bridge will delay for a period to become edge port if no bridge BPUD is received. The default is auto mode.
p2p - (Optional) To decide if this port is in Full-Duplex or Half-Duplex mode. **true** - Specify that the port(s) is in Full-Duplex mode. **false** - Specify that the port(s) is in Half-Duplex mode. **auto** - Specify that the port(s) is in Full-Duplex and Half-Duplex mode.
state - (Optional) To decide if this port supports the STP functionality. **enable** - Specify that STP functionality on the port(s) is enabled. **disable** - Specify that STP functionality on the port(s) is disabled.
restricted_role - (Optional) To decide if this port not to be selected as Root Port. The default value is false. **true** - Specify that the port can be specified as the root port. **false** - Specify that the port can not be specified as the root port.
restricted_tcn - (Optional) To decide if this port not to propagate topology change. The default value is false. **true** - Specify that the port can be set to propagate a topology change. **false** - Specify that the port can not be set to propagate a topology change.
fbpdu - (Optional) To decide if this port will flood STP BPDU when STP functionality is disabled. When the state is set to enable, the received BPDU will be forwarded. When the state is set to disable, the received BPDU will be dropped. **enable** - Specify that the port can be set to flood the STP BPDU when the STP functionality is disabled. **disable** - Specify that the port can not be set to flood the STP BPDU when the STP functionality is disabled.

Restrictions

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

Example

To configure STP ports:

```
DES-3200-28P:admin#config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

DES-3200-28P:admin#
```

46-12 show stp ports

Description

This command is used to show the port information includes parameters setting and operational value.

Format

show stp ports {<portlist>}

Parameters

ports - To show parameters of the designated port numbers, to be distinguished from showing parameters of the bridge. **<portlist>** - (Optional) Enter a list of ports used for the configuration here.

Restrictions

None.

Example

To show STP ports:

```
DES-3200-28P:admin#show stp ports
Command: show stp ports

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









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

46-13 config stp priority

Description

This command is used to configure the instance priority.

Format

config stp priority <value 0-61440> instance_id <value 0-7>

Parameters

priority - Specify the bridge priority value. This value must be divisible by 4096. **<value 0-61440>** - Enter the bridge priority value here. This value must be between 0 and 61440.
instance_id - Identifier to distinguish different STP instances. **<value 0-7>** - Enter the STP instance ID here. This value must be between 0 and 7.

Restrictions

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

Example

To configure the STP instance ID:

```
DES-3200-28P:admin#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DES-3200-28P:admin#
```

46-14 config stp version

Description

This command is used to enable STP globally.

Format

config stp version [mstp | rstp | stp]

Parameters

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

Example

To configure STP version:

```
DES-3200-28P:admin#config stp version mstp
Command: config stp version mstp

Success.

DES-3200-28P:admin#
```

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

```
DES-3200-28P:admin#config stp version mstp
Command: config stp version mstp

Configure value is the same with current value.
Success.

DES-3200-28P:admin#
```

46-15 show stp instance

Description

This command is used to display each instance parameters settings. Value means the instance ID, if there is no input of this value, all instance will be shown.

Format

show stp instance {<value 0-7>}

Parameters

instance - Specify the MSTP instance ID.
<value 0-7> - (Optional) Enter the MSTP instance ID value here. This value must be between 0 and 7.

Restrictions

None.

Example

To show STP instance:

```
DES-3200-28P:admin#show stp instance
Command: show stp instance

STP Instance Settings
---------------------------
Instance Type          : CIST
Instance Status        : Enabled
Instance Priority      : 32768(bridge priority : 32768, sys ID ext : 0 )

STP Instance Operational Status
-------------------------------
Designated Root Bridge : 32768/00-22-22-22-22-00
External Root Cost     : 0
Regional Root Bridge   : 32768/00-22-22-22-22-00
Internal Root Cost     : 0
Designated Bridge      : 32768/00-22-22-22-22-00
Root Port                : None
Max Age                  : 20
Forward Delay           : 15
Last Topology Change   : 2430
Topology Changes Count : 0

DES-3200-28P:admin#
```

Chapter 47 Network Load Balancing (NLB) Command List

create nlb unicast_fdb <macaddr>
config nlb unicast_fdb <macaddr>[add|delete]<portlist>
delete nlb unicast_fdb <macaddr>
create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>
delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
show nlb fdb

47-1 create nlb unicast_fdb

Description

This command is used to create the NLB unicast FDB entry.

The network load balancing command set is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. The server can work in two different modes – unicast mode and multicast mode. In unicast mode, the client use unicast MAC address as the destination MAC to reach the server. In multicast mode, the client use the multicast MAC address as the destination MAC to reach the server. Regarding of the mode, this destination Mac is the named the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet.

Format

create nlb unicast_fdb <macaddr>

Parameters

<macaddr> - Specify the MAC address of the NLB unicast FDB entry to be created.

Restrictions

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

Example

To create an NLB unicast MAC forwarding entry, for the product that support the VLAN information on the unicast forwarding:

```
DES-3200-28P:admin#create nlb unicast_fdb 02-bf-01-01-01-01
Command: create nlb unicast_fdb 02-BF-01-01-01-01

Success.

DES-3200-28P:admin#
```

47-2 config nlb unicast_fdb

Description

This command is used to add or delete the forwarding ports for the specified NLB unicast FDB entry.

Format

config nlb unicast_fdb <macaddr>[add|delete]<portlist>

Parameters

<macaddr> - Specify the MAC address of the NLB unicast FDB entry to be configured.
add - Specify to add the ports.
delete - Specify to delete the ports.
<portlist> - Specify a list of forwarding ports to be added or removed.

Restrictions

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

Example

To configure NLB unicast FDB entry, for the product that support the VLAN information on the unicast forwarding:

```
DES-3200-28P:admin#config nlb unicast_fdb 02-bf-01-01-01-01 add 1-5
Command: config nlb unicast_fdb 02-BF-01-01-01-01 add 1-5

Success.

DES-3200-28P:admin#
```

47-3 delete nlb unicast_fdb

Description

This command is used to delete the NLB unicast FDB entry.

Format

delete nlb unicast_fdb <macaddr>

Parameters

<macaddr> - Specify the MAC address of the NLB unicast FDB entry to be deleted.

Restrictions

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

Example

To delete the NLB unicast FDB entry, for the product that support the VLAN information on the unicast forwarding:

```
DES-3200-28P:admin#delete nlb unicast_fdb 02-bf-01-01-01-01
Command: delete nlb unicast_fdb 02-BF-01-01-01-01

Success.

DES-3200-28P:admin#
```

47-4 create nlb multicast_fdb

Description

This command is used to create a NLB multicast FDB entry.

The NLB multicast FDB entry will be mutual exclusive with the L2 multicast entry.

Format

create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>

Parameters

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specify the VLAN by the VLAN ID. **<vlanid>** - Enter the VLAN ID here.
<macaddr> - Specify the MAC address of the NLB multicast FDB entry to be created.

Restrictions

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

Example

To create a NLB multicast FDB entry:

```
DES-3200-28P:admin#create nlb multicast_fdb default 03-bf-01-01-01-01
Command: create nlb multicast_fdb default 03-bf-01-01-01-01

Success.

DES-3200-28P:admin#
```

47-5 config nlb multicast_fdb

Description

This command is used to add or delete the forwarding ports for the specified NLB multicast FDB entry.

Format

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

Parameters

<vlan_name 32> - Specify the VLAN of the NLB multicast FDB entry to be configured.
vlanid - Specify the VLAN by the VLAN ID. **<vlanid>** - Enter the VLAN ID here.
<macaddr> - Specify the Mac address of the NLB multicast FDB entry to be configured.
add - Specify a list of forwarding ports to be added.
delete - Specify a list of forwarding ports to be deleted.
<portlist> - Enter the list of ports used for this configuration.

Restrictions

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

Example

To configure NLB multicast MAC forwarding database:

```
DES-3200-28P:admin#config nlb multicast_fdb default 03-bf-01-01-01-01 add 1-5
Command: config nlb multicast_fdb default 03-bf-01-01-01-01 add 1-5

Success.

DES-3200-28P:admin#
```

47-6 delete nlb multicast_fdb

Description

This command is used to delete the NLB multicast FDB entry.

Format

delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>

Parameters

<vlan_name 32> - Specify the VLAN of the NLB multicast FDB entry to be deleted.
vlanid - Specify the VLAN by VLAN ID. **<vlanid>** - Enter the VLAN ID here.
<macaddr> - Specify the MAC address of the NLB multicast FDB entry to be deleted.

Restrictions

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

Example

To delete NLB multicast FDB entry:

```
DES-3200-28P:admin#delete nlb multicast_fdb default 03-bf-01-01-01-01
Command: delete nlb multicast_fdb default 03-bf-01-01-01-01

Success.

DES-3200-28P:admin#
```

47-7 show nlb fdb

Description

This command is used to show the NLB Configured entry.

Format

show nlb fdb

Parameters

None.

Restrictions

None.

Example

To display the NLB forwarding table:

```
DES-3200-28P:admin#show nlb fdb
Command: show nlb fdb

 MAC Address       VLAN ID    Egress Ports
 ----------------- ---------- ------------------------------------------------
 02-BF-01-01-01-01 -          1-5

Total Entries :1

DES-3200-28P:admin#
```

Chapter 48 Network Monitoring Command List

show packet ports <portlist>
show error ports <portlist>
show utilization [cpu | ports]
show utilization dram
show utilization flash
clear counters {ports <portlist>}

48-1 show packet ports

Description

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

Format

show packet ports <portlist>

Parameters

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

Restrictions

None.

Example

To display the packets analysis for port 7:

```
DES-3200-28P:admin#show packet ports 7
Command: show packet ports 7

 Port Number : 7
 ================================================================
 Frame Size/Type       Frame Counts                Frames/sec
 ---------------       ----------------------      -----------
 64                    0                           0
 65-127                0                           0
 128-255               0                           0
 256-511               0                           0
 512-1023              0                           0
 1024-1518             0                           0
 Unicast RX            0                           0
 Multicast RX          0                           0
 Broadcast RX          0                           0

 Frame Type            Total                       Total/sec
 ---------------       ----------------------      -----------
 RX Bytes              0                           0
 RX Frames             0                           0
 TX Bytes              0                           0
 TX Frames             0                           0


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

48-2 show error ports

Description

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

Format

show errors ports <portlist>

Parameters

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

Restrictions

None.

Example

To display the errors of the port:

```
DES-3200-28P:admin#show error ports 3
Command: show error ports 3


 Port Number : 3
                RX Frames                                   TX Frames
                ---------                                   ---------
 CRC Error      0                    Excessive Deferral     0
 Undersize      0                    CRC Error              0
 Oversize       0                    Late Collision         0
 Fragment       0                    Excessive Collision    0
 Jabber         0                    Single Collision       0
 Drop Pkts      0                    Collision              0
 Symbol Error   0




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

48-3 show utilization

Description

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

Format

show utilization [cpu | ports]

Parameters

cpu - Specify to display information regarding the CPU.
ports - Specify all ports to be displayed.

Restrictions

None.

Example

To display the ports utilization:

```
DES-3200-28P:admin#show utilization ports
Command: show utilization ports

 Port     TX/sec     RX/sec   Util      Port     TX/sec     RX/sec   Util
 -----  ---------- ---------- ----      -----  ---------- ---------- ----
 1      0          0          0         21     0          0          0
 2      0          0          0         22     0          0          0
 3      0          0          0         23     0          0          0
 4      0          0          0         24     0          0          0
 5      0          0          0         25     0          0          0
 6      0          0          0         26     0          0          0
 7      0          0          0         27     0          0          0
 8      0          0          0         28     0          0          0
 9      0          0          0
 10     0          0          0
 11     0          0          0
 12     0          0          0
 13     0          0          0
 14     0          0          0
 15     0          0          0
 16     0          0          0
 17     0          0          0
 18     0          0          0
 19     0          0          0
 20     0          0          0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the CPU utilization:

```
DES-3200-28P:admin#show utilization cpu
Command: show utilization cpu

CPU Utilization
-------------------------------------------------------------------------------
Five seconds -  10 %         One minute -  10 %         Five minutes -  10 %









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

48-4 show utilization dram

Description

This command is used to show DRAM memory utilization.

Format

show utilization dram

Parameters

None.

Restrictions

None.

Example

To display DRAM utilization:

```
DES-3200-52P:admin#show utilization dram
Command: show utilization dram

DRAM Utilization :
        Total DRAM      : 131072    KB
        Used DRAM       : 115758    KB
        Utilization     : 88 %



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

48-5 show utilization flash

Description

This command is used to show the flash memory utilization.

Format

show utilization flash

Parameters

None.

Restrictions

None.

Example

To display FLASH utilization:

```
DES-3200-52P:admin#show utilization flash
Command: show utilization flash

Flash Memory Utilization :
        Total Flash     : 29618     KB
        Used Flash      : 5553      KB
        Utilization     : 18 %


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

48-6 clear counters

Description

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

Format

clear counters {ports <portlist>}

Parameters

ports - (Optional) Specify a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separeted by a colon) are specified. The beginning and end of the port list range are seperated by a dash. **<portlist>** - Enter a list of ports used for the configuration here.
If no parameter is specified, system will display counters of all the ports .

Restrictions

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

Example

To clear the Switch's statistics counters:

```
DES-3200-28P:admin#clear counters ports 7-9
Command: clear counters ports 7-9

Success.

DES-3200-28P:admin#
```

Chapter 49 OAM Commands

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]}(1) | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}(1)]| critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]
show ethernet_oam ports {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]
clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

49-1 config ethernet_oam ports

Description

This command is used to configure Ethernet OAM. The parameter to configure port Ethernet OAM mode operates in active or passive mode. The following two actions are allowed by ports in active mode, but disallowed by ports in passive mode: Initiate OAM discovery and start or stop remote loopback. Note that when a port is OAM-enabled, changing the OAM mode will cause the OAM discovery to be re-started.

The command used to enable or disable port's Ethernet OAM function. The parameter enabling a port's OAM will cause the port to start OAM discovery. If a port's is active, it initiates the discovery. Otherwise it reacts to the discovery received from peer. Disabling a port's OAM will cause the port to send out a dying gasp event to peers and then disconnect the established OAM link.

The link monitoring parameter is used to configure port Ethernet OAM link monitoring error symbols. The link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of symbol errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error symbol period event to notify the remote OAM peer. The Ethernet OAM link monitoring error frames parameter provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counter on the number of frame errors as well as the number of coding symbol errors. When the number of frame errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame event to notify the remote OAM peer.

The link event parameter configures the capability of the Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event. The command is used to configure the client to process or to ignore the received Ethernet OAM remote loopback command. In remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback command will prevent the port from entering remote loopback mode.

Format

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]}(1) | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}(1)]| critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]

Parameters

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

all - Used to specify all ports are to be configured.

mode - Specify the operation mode. The default mode is active.
- **active** - Specify to operate in active mode.
- **passive** - Specify to operate in passive mode.

state - Specify the OAM function status.
- **enable** - Specify to enable the OAM function.
- **disable** - Specify to disable the OAM function.

link_monitor - Used to detect and indicate link faults under a variety of conditions.
- **error_symbol** - Used to generate an error symbol period event to notify the remote OAM peer.
  - **threshold** - Specify the number of symbol errors in the period that is required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 symbol error.
    - **<range 0-4294967295>** - Specify the range from 0 to 4294967295.
  - **window** - The range is 1000 to 60000 ms. The default value is 1000ms.
    - **<millisecond 1000-60000>** -The range is 1000 to 60000 ms.
  - **notify_state** - Specify the event notification status. The default state is enable.
    - **enable** -Specify to enable event notification.
    - **disable** -Specify to disable event notification.
- **error_frame** - Specify the error frame.
  - **threshold** - Specify a threshold range.
    - **<range 0-4294967295>** - Specify a threshold range between 0 and 4294967295.
  - **window** - The range is 1000 to 60000 ms. The default value is 1000ms.
    - **<millisecond 1000-60000>** - The range is 1000 to 60000 ms.
  - **notify_state** - Specify the event notification status. The default state is enable.
    - **enable** - Specify to enable event notification.
    - **disable** - Specify to disable event notification.
- **error_frame_seconds** - Specify error fram time.
  - **threshold** - Specify a threshold range between 1 and 900.
    - **<range 1-900>** -Specify a threshold range between 1 and 900.
  - **window** - The range is 1000 to 900000 ms.
    - **<millisecond 10000-900000>** - The range is 1000 to 900000 ms.
  - **notify_state** - Specify the event notification status. The default state is enable.
    - **enable** - Specify to enable event notification.
    - **disable** - Specify to disable event notification.
- **error_frame_period** - Specify error frame period.
  - **threshold** - Specify a threshold range between 0 and 4294967295.
    - **<range 0-4294967295>** -Specify a threshold range between 0 and 4294967295.
  - **window** - The range is 148810 to 100000000 ms.
    - **<number 148810-100000000>** - The range is 148810 to 100000000 ms.
  - **notify_state** - Specify the event notification status. The default state is enable.
    - **enable** - Specify to enable event notification.
    - **disable** - Specify to disable event notification.

critical_link_event –Specify critical link event. **dying_gasp** - An unrecoverable local failure condition has occurred. **critical_event** - An unspecified critical event has occurred. **notify_state** - Specify the event notification status. The default state is enable. **enable** - Specify to enable event notification. **disable** - Specify to disable event notification.
remote_loopback - Specify remote loop. **start** - If start is specified, it will request the peer to change to the remote loopback mode. **stop** - If stop is specified, it will request the peer to change to the normal operation mode.
received_remote_loopback - Specify receive remote loop-back. **process** - Specify to process the received Ethernet OAM remote loopback command. **ignore** - Specify to ignore the received Ethernet OAM remote loopback command. The default method is"ignore".

Restrictions

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

Example

To configure Ethernet OAM on ports 1 to 2 in active mode:

```
DES-3200-28P:admin#config ethernet_oam ports 1-2 mode active
Command: config ethernet_oam ports 1-2 mode active

Success.

DES-3200-28P:admin#
```

To enable Ethernet OAM on port 1:

```
DES-3200-28P:admin#config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.

DES-3200-28P:admin#
```

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DES-3200-28P:admin#config ethernet_oam ports 1 link_monitor error_symbol
threshold 2 window 1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_symbol threshold 2
window 1000 notify_state enable

Success.

DES-3200-28P:admin#
```

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DES-3200-28P:admin#config ethernet_oam ports 1 link_monitor error_frame
threshold 2 window 1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame threshold 2
window 1000 notify_state enable

Success.

DES-3200-28P:admin#
```

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DES-3200-28P:admin#config ethernet_oam ports 1 link_monitor error_frame_seconds
threshold 2 window 10000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_seconds threshold
2 window 10000 notify_state enable

Success.

DES-3200-28P:admin#
```

To configure the error frame threshold to10 and period to 1000000 ms for port 1:

```
DES-3200-28P:admin#config ethernet_oam ports 1 link_monitor error_frame_period
threshold 10 window 1000000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_period threshold
10 window 1000000 notify_state enable

Success.

DES-3200-28P:admin#
```

To configure a dying gasp event for port 1:

```
DES-3200-28P:admin#config ethernet_oam ports 1 critical_link_event dying_gasp
notify_state enable
Command: config ethernet_oam ports 1 critical_link_event dying_gasp
notify_state enable

Success.

DES-3200-28P:admin#
```

To start remote loopback on port 1:

```
DES-3200-28P:admin#config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.

DES-3200-28P:admin#
```

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DES-3200-28P:admin#config ethernet_oam ports 1 received_remote_loopback process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success.

DES-3200-28P:admin#
```

49-2 show ethernet_oam ports

Description

This command is used to display Ethernet OAM information, including status, configuration, statistics, and event log, on specified ports.

The status information includes:

(1) OAM administration status: enabled or disabled.

(2) OAM operation status. It maybe the below value:

- Disable: OAM is disabled on this port.
- LinkFault: The link has detected a fault and is transmitting OAMPDUs with a link fault indication.
- PassiveWait: The port is passive and is waiting to see if the peer device is OAM capable.
- ActiveSendLocal: The port is active and is sending local information.
- SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.
- SendLocalAndRemoteOk: The local device agrees the OAM peer entity.
- PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity.
- PeeringRemotelyRejected: The remote OAM entity rejects the local device.
- Operational: The local OAM entity learns that both it and the remote OAM entity have accepted the peering.
- NonOperHalfDuplex: Since Ethernet OAM functions are not designed to work completely over half-duplex port. This value indicates Ethernet OAM is enabled but the port is in half-duplex operation.

(3) OAM mode: passive or active.

(4) Maximum OAMPDU size: The largest OAMPDU that the OAM entity supports. OAM entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU sizes between the peers.

(5) OAM configuration revision: The configuration revision of the OAM entity as reflected in the latest OAMPDU sent by the OAM entity. The config revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed.

(6) OAM mode change.

(7) OAM Functions Supported: The OAM functions supported on this port. These functions include:

1. Unidirectional: It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).
2. Loopback: It indicates that the OAM entity can initiate and respond to loopback commands.
3. Link Monitoring: It indicates that the OAM entity can send and receive Event Notification OAMPDUs.
4. Variable: It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB.

The event log displays Ethernet OAM event log information. The switch can buffer 1000 event logs. The event log is different from sys-log as it provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog.

Format

show ethernet_oam ports {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]

Parameters

<portlist> - (Optional) Specify the range of ports to display.
status - Specify to display the Ethernet OAM status.
configuration - Specify to display the Ethernet OAM configuration.
statistics - Specify to display Ethernet OAM statistics.
event_log - Specify to display the Ethernet OAM event log information. **index** - (Optional) Specify an index range to display. **<value_list>** - (Optional) Specify an index range to display.

Restrictions

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

Example

To display Ethernet OAM statistics information for port 1:

```
DES-3200-28P:admin#show ethernet_oam ports 1 statistics
Command: show ethernet_oam ports 1 statistics

Port 1
------------------------------------------------------------
Information OAMPDU TX                : 0
Information OAMPDU RX                : 0
Unique Event Notification OAMPDU TX   : 0
Unique Event Notification OAMPDU RX   : 0
Duplicate Event Notification OAMPDU TX: 0
Duplicate Event Notification OAMPDU RX: 0
Loopback Control OAMPDU TX            : 0
Loopback Control OAMPDU RX            : 0
Variable Request OAMPDU TX            : 0
Variable Request OAMPDU RX            : 0
Variable Response OAMPDU TX           : 0
Variable Response OAMPDU RX           : 0
Organization Specific OAMPDUs TX      : 0
Organization Specific OAMPDUs RX      : 0
Unsupported OAMPDU TX                 : 0
Unsupported OAMPDU RX                 : 0
Frames Lost Due To OAM                : 0

DES-3200-28P:admin#
```

49-3 clear ethernet_oam ports

Description

This command is used to clear Ethernet OAM information.

Format

clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

Parameters

<portlist> - Specify a range of Ethernet OAM ports to be cleared.
all - Specify to clear all Ethernet OAM ports.
event_log - Specify to clear Ethernet OAM event log information.
statistics - Specify to clear Ethernet OAM statistics.

Restrictions

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

Example

To clear port 1 OAM statistics:

```
DES-3200-28P:admin#clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.

DES-3200-28P:admin#
```

To clear port 1 OAM events:

```
DES-3200-28P:admin#clear ethernet_oam ports 1 event_log
Command: clear ethernet_oam ports 1 event_log

Success.

DES-3200-28P:admin#
```

Chapter 50 Peripherals Command List

show device_status
show environment
config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}
config temperature [trap | log] state [enable | disable]

50-1 show device_status

Description

This command is used to display current status of power(s) and fan(s) on the system.

Within fan(s) status display, for example, there are three fans on the left of the Switch, if three fans is working normally, there will display “OK” in the Left Fan field. If some fans work failed, such as fan 1,3 , there will only display the failed fans in the Left Fan field, such as “1,3 Fail”.

In the same way, the Right Fan, Back Fan is same to Left Fan. Because there is only one CPU Fan, if it is working failed, display “Fail”, otherwise display “OK”.

Format

show device_status

Parameters

None.

Restrictions

None.

Example

To show device status:

```
DES-3200-28P:admin#show device_status
Command: show device_status

    Internal Power: OK
    External Power: None
    Right Fan     : OK

DES-3200-28P:admin#
```

50-2 show environment

Description

This command is used to display current status of power(s) and fan(s) on the system.

Format

show environment

Parameters

None.

Restrictions

None.

Example

To display the device environment:

```
DES-3200-28P:admin#show environment
Command: show environment

Temperature Trap State      : Enabled
Temperature Log State       : Enabled
Internal Power      : Active
External Power      : None
Current Temperature(Celsius) :   32
High Warning Temperature Threshold(Celsius) :    79
Low Warning Temperature Threshold(Celsius)  :    11

DES-3200-28P:admin#
```

50-3 config temperature threshold

Description

This command is used to configure the warning threshold for high and low temperature.

Format

config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}

Parameters

threshold - Specify the high and low threshold value.
- **high** - (Optional) To configure high threshold value. The high threshold must bigger than the low threshold.
  - **<temperature -500-500>** - Enter the high threshold temperature.
- **low** - (Optional) To configure low threshold value.
  - **<temperature -500-500>** - Enter the low threshold temperature.

Restrictions

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

Example

To configure the warning temperature threshold:

```
DES-3200-28P:admin#config temperature threshold high 80
Command: config temperature threshold high 80

Success.

DES-3200-28P:admin#
```

50-4 config temperature

Description

This command is used to configure the trap state for temperature warning event.

Format

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

Parameters

trap state - Specify the trap state for the warning temperature event. **enable** - Enable trap state for warning temperature event. The default state is enabled. **disable** - Disable trap state for warning temperature event.
log state - Specify the log state for the warning temperature event. **enable** - Enable log state for warning temperature event. The default state is enabled. **disable** - Disable log state for warning temperature event.

Restrictions

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

Example

To configure the warning temperature trap state:

```
DES-3200-28P:admin#config temperature trap state enable
Command: config temperature trap state enable

Success.

DES-3200-28P:admin#
```

Chapter 51 Ping Command List

ping <ipaddr> {times <value 1-255> | timeout <sec 1-99>}
ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99>}

51-1 ping

Description

This command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the Switch and the remote device.

Format

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

Parameters

<ipaddr> - Specify the IP address of the host.
times - (Optional) The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0, indicating infinity. Press the "CTRL+C” to break the ping test. **<value 1-255>** - Enter the number of individual ICMP echo messages to be sent here. This value must be between 1 and 255.
timeout - (Optional) Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second. **<sec 1-99>** - Enter the time-out period here. This value must be between 1 and 99 seconds.

Restrictions

None.

Example

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

```
DES-3200-28P:admin#ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms

Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

DES-3200-28P:admin#
```

51-2 ping6

Description

This command is used to send IPv6 Internet Control Message Protocol (ICMP) echo messages to a remote IPv6 address. The remote IPv6 address will then “echo” or return the message. This is used to confirm the IPv6 connectivity between the Switch and the remote device.

Format

ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99>}

Parameters

<ipv6addr> - Enter the IPv6 address here.
times - (Optional) The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0, indicating infinity. Press the "CTRL+C” to break the ping test. **<value 1-255>** - Enter the number of individual ICMP echo messages to be sent here. This value must be between 1 and 255.
size - (Optional) Size of the test packet. **<value 1-6000>** - Enter the size of the test packet here. This value must be between 1 and 6000.
timeout - (Optional) Defines the time-out period while waiting for a response from the remote device. **<sec 1-99>** - Enter the time-out period here. This value must be between 1 and 99 seconds. The default is 1 second.

Restrictions

None.

Example

To send ICMP echo message to “3000::1” for 4 times:

```
DES-3200-28P:admin#ping6 3000::1 times 4
Command: ping6 3000::1 times 4

Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms

Ping Statistics for 3000::1
Packets: Sent =4, Received =4, Lost =0

DES-3200-28P:admin#
```

Chapter 52 Port Security Command List

config port_security system max_learning_addr [<max_lock_no 1-3328> | no_limit]
config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3328> | lock_address_mode [permanent | deleteontimeout | deleteonreset]} (1)| {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]}(1)]
config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]
delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>
clear port_security_entry {ports [<portlist> | all] {[vlan <vlan_name 32> | vlanid <vidlist>]}}
show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}
show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}
enable port_security trap_log
disable port_security trap_log

52-1 config port_security system max_learning_addr

Description

This command is used to set the maximum number of port security entries that can be authorized system wide.

There are four levels of limitations on the learned entry number; for the entire system, for a port, for a VLAN, and for a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

The setting for system level maximum learned users must be greater than the total of maximum learned users allowed on all ports.

Format

config port_security system max_learning_addr [<max_lock_no 1-3328> | no_limit]

Parameters

<max_lock_no 1-3328> - Specify the maximum number of port security entries that can be learned by the system. If the setting is smaller than the number of current learned entries on all enabled ports, the command will be rejected. This value must be between 1 and 3328.
no_limit - No limitation on the number of port security entries that can be learned by the system. By default, the number is set to no_limit.

Restrictions

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

Example

To configure the maximum number of port security entries on the Switch to be 256:

```
DES-3200-28P:admin#config port_security system max_learning_addr 256
Command: config port_security system max_learning_addr 256

Success.

DES-3200-28P:admin#
```

52-2 config port_security ports

Description

This command is used to configure the admin state, the maximum number of addresses that can be learnt and the lock address mode.

There are four levels that limit the number of learned entries; the entire system, a port, a VLAN, and a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

Format

config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr < max_lock_no 0-3328> | lock_address_mode [permanent | deleteontimeout | deleteonreset]} (1)| {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]}(1)]

Parameters

<portlist> - Enter the list of port used for this configuration here.
all - Specify that all ports will be configured.
admin_state - (Optional) Specify the state of the port security function on the port. **enable** - Specify to enable the port security function on the port. **disable** - Specify to disable the port security function on the port. By default, the setting is disabled.
max_learning_addr - (Optional) Specify the maximum number of port security entries that can be learned on this port. If the value is set to 0, it means that no user can be authorized by the port security function on this port. If the setting is smaller than the number of current learned entries on the port, the command will be rejected. The default value is 32. **<max_lock_no 0-3328>** - Enter the maximum number of port security entries that can be learned here. This value must be between 0 and 3328.
lock_address_mode - (Optional) Indicates the lock address mode. The default mode is deleteonreset. **permanent** - The address will never be deleted unless the user removes it manually, the VLAN of the entry is removed, the port is removed from the VLAN, or port security is disabled on the port where the address resides. **deleteontimeout** - This entry will be removed if the entry is idle for the specified aging time. **deleteonreset** - This address will be removed if the Switch is reset or rebooted. Events that cause permanent entries to be deleted also apply to the deleteonreset entries.
vlan - (Optional) Specify the VLAN name used here. **<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long. **vlanid** - (Optional) Specify the VLAN ID used here. **<vidlist>** - Enter the VLAN ID used here.
max_learning_addr - (Optional) Specify the maximum learning address value. **<max_lock_no 0-3328>** - Enter the maximum learning address value here. This value must be between 0 and 3328. **no_limit** - Specify that the maximum learning address value will be set to no limit.

Restrictions

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

Example

To configure the port-based port security setting so that the maximum number of port security entries is restricted to 10, and the lock_address mode is set to permanent on port 6:

```
DES-3200-28P:admin#config port_security ports 6 admin_state enable
max_learning_addr 10 lock_address_mode permanent
Command: config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode permanent

Success.

DES-3200-28P:admin#
```

52-3 config port_security vlan

Description

This command is used to set the maximum number of port security entries that can be learned on a specific VLAN.

There are four levels that limit the number of learned entries; the entire system, a port, a VLAN, and a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

Format

config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]

Parameters

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specify a list of VLANs by VLAN ID. **<vidlist>** - Enter the VLAN ID list here.
max_learning_addr - Specify the maximum number of port security entries that can be learned by this VLAN. If this parameter is set to 0, it means that no user can be authorized on this VLAN. If the setting is lower than the number of current learned entries on the VLAN, the command will be rejected. The default value is “no_limit” **<max_lock_no 0-3328>** - Enter the maximum number of port security entries that can be learned here. This value must be between 0 and 3328. **no_limit** - No limitation on the number of port security entries that can be learned by a specific VLAN.

Restrictions

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

Example

To configure the maximum number of VLAN-based port security entries on VLAN 1 to be 64:

```
DES-3200-28P:admin#config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

DES-3200-28P:admin#
```

52-4 delete port_security_entry

Description

This command is used to delete a port security entry.

Format

delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>

Parameters

vlan - Specify the VLAN by VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specify the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID list here. This value must be between 1 and 4094.
mac_address - Specify the MAC address of the entry. **<macaddr>** - Enter the MAC address used here.

Restrictions

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

Example

To delete the port security entry with a MAC address of 00-00-00-00-00-01 on VLAN 1:

```
DES-3200-28P:admin#delete port_security_entry vlanid 1 mac_address 00-00-00-00-
00-01
Command: delete port_security_entry vlanid 1 mac_address 00-00-00-00-00-01

Success.

DES-3200-28P:admin#
```

52-5 clear port_security_entry

Description

This command is used to clear the MAC entries learned by the port security function.

Format

clear port_security_entry {ports [<portlist> | all] {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specify the range of ports to be configured. **<portlist>** - The port security entries learned on the specified port will be cleared. **all** - All the port security entries learned by the system will be cleared.
vlan - (Optional) The port security entries learned on the specified VLANs will be cleared. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specify a list of VLANs by VLAN ID. **<vidlist>** - Enter the VLAN ID list here.

Restrictions

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

Example

To clear the port security entries on port 6:

```
DES-3200-28P:admin#clear port_security_entry ports 6
Command: clear port_security_entry ports 6

Success.

DES-3200-28P:admin#
```

52-6 show port_security_entry

Description

This command is used to display the port security entries.

If more than one parameter is selected, only the entries matching all the selected parameters will be displayed.

If the user specifies ports and VLAN (either the VLAN name or VLAN ID list), only the entries matching all the parameters will be displayed.

Format

show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specify the range of ports that will display the port security entries. While this parameter is null, to show the entries on all of the ports. **<portlist>** - Enter the list of port used for this configuration here.
vlan - (Optional) Specify the name of the VLAN that the port security settings will be displayed for. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN that the port security entries will be displayed for. **<vidlist>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To show all the port security entries:

```
DES-3200-28P:admin#show port_security_entry
Command: show port_security_entry

MAC Address          VID   Port   Lock Mode
-----------------  ----  -----  ---------------
00-00-00-00-00-01  1      25     DeleteOnTimeout

Total Entries: 1

DES-3200-28P:admin#
```

52-7 show port_security

Description

This command is used to display the port security related information, including state, maximum learned addresses and lock address mode on a port and/or on a VLAN.

If both ports and vlanid (or vlan_name) are specified, configurations matching any of these parameters will be displayed.

Format

show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specify the range of ports that will show their configuration. While this parameter is null, to show the entries on all of the ports. **<portlist>** - Enter the list of port used for this configuration here.
vlan - (Optional) Specify the name of the VLAN that will show its configuration. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specify the ID of the VLAN that will show its configuration. **<vidlist>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the global configuration of port security:

```
DES-3200-28P:admin#show port_security
Command: show port_security

 Port Security Trap/Log        : Disabled
 System Maximum Address        : 256

 VLAN Configuration (Only VLANs with limitation are displayed)
 VID   VLAN Name                         Max. Learning Addr.
 ----  --------------------------------  ------------------
 1     default                           64

DES-3200-28P:admin#
```

52-8 enable port_security trap_log

Description

This command is used to enable port security traps/logs. When this command is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out with the MAC and port information and the relevant information will be logged.

Format

enable port_security trap_log

Parameters

None.

Restrictions

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

Example

To enable a port security trap:

```
DES-3200-28P:admin#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3200-28P:admin#
```

52-9 disable port_security trap_log

Description

This command is used to disable a port security trap/log. If the port security trap is disabled, no trap will be sent out for MAC violations, and no log will be recorded.

Format

disable port_security trap_log

Parameters

None.

Restrictions

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

Example

To prevent a port security trap from being sent from the switch:

```
DES-3200-28P:admin#disable port_security trap_log
Command: disable port_security trap_log

Success.

DES-3200-28P:admin#
```

Chapter 53 Power over Ethernet (PoE) Command List (DES-3200-28P and DES-3200-52P Only)

config poe system {power_limit <value 37-188> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]} **(DES-3200-28P Only)**
config poe system {power_limit <value 37-370> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]} **(DES-3200-52P Only)**
config poe ports [all | <portlist>] { state [enable | disable]| [time_range <range_name 32> | clear_time_range]| priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-35000>]}
show poe system
show poe ports {<portlist>}

53-1 config poe system

Description

This command is used to configure the parameters for the POE system-wise function.

Format

config poe system {power_limit <value 37-188> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]} (DES-3200-28P Only)

config poe system {power_limit <value 37-370> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]} (DES-3200-52P Only)

Parameters

power_limit - (Optional) Configure the power budget of PoE system. The range of value which can be specified is determined by the system. **<value 37-188>** - Enter the power limit value here. This value must be between 37 and 188. **(DES-3200-28P Only)** **<value 37-370>** - Enter the power limit value here. This value must be between 37 and 370. **(DES-3200-52P Only)**
power_disconnect_method - (Optional) Configure the disconnection method that will be used when the power budget is running out. When the system attempts to supply power to a new port, if the power budget is insufficient to do this, PoE controller will initiate port disconnection procedure to prevent overloading the power supply. The controller uses one of the following two ways to perform the disconnection procedure. **deny_next_port** - The port with max port number will be denied regardless of its priority. Note that if the disconnect_method is set to deny_next_port, then the power provision will not utilize the system's maximum power. There is a 19W safe margin. That is, when the system has only 19W remaining, this power cannot be utilized. **deny_low_priority_port** - If there are ports that have been supplied power that have a priority lower than the new port, the port with the lowest priority will be disconnected. This process will stop until enough power is released for the new port. Note that if the

disconnect_method is set to deny_low_priority_port, then the power provision can utilize the system's maximum power.
legacy_pd - Configure legacy PDs detection status, enable for support, if set to disable, can't detect legacy PDs signal. **enable** - Specify that the legacy PDs detection status will be enabled. **disable** - Specify that the legacy PDs detection status will be disabled.

Restrictions

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

Example

To config PoE system-wise was setting:

```
DES-3200-28P:admin#config poe system power_limit 150 power_disconnect_method
deny_low_priority_port
Command: config poe system power_limit 150 power_disconnect_method
deny_low_priority_port

Success.

DES-3200-28P:admin#
```

53-2 config poe ports

Description

This command is used to configure the PoE port settings.

Based on 802.3af, there are 5 kinds of PD classes, class 0, class 1, class 2, and class 3. The power consumption ranges for them are 0.44~12.95W, 0.44~3.84W, 3.84~6.49W, 6.49~12.95W, and 12.95~ 29.5W, respectively.

The five pre-defined settings are for users' convenience: The following is the power limit applied to the port for these four classes. For each class, the power limit is a little more than the power consumption range for the class. This takes the factor of the power loss on cable into account. Thus, the following are the typical values defined by the chip vendor.

Class 0: 15400mW

Class 1: 4000mW

Class 2: 7000mW

Clase 3: 15400mW

Other than these four pre-defined settings, users can directly specify any value that the chip supported, Normally, the minimum setting is 1000mW, and the maximum setting is 15400mW for 802.3af and >=35000mW for 802.3at.

Format

config poe ports [all | <portlist>] { state [enable | disable] | [time_range <range_name 32> | clear_time_range] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-35000>]}

Parameters

ports - Specify the list of ports whose setting is under configuration. **all** - Specify that all the ports will be included in this configuration. **<portlist>** - Enter the list of port used for this configuration here.
state - (Optional) When the state is set to disable, power will not be supplied to the powered device connected to this port. **enable** - Specify that state will be enabled. **disable** - Specify that state will be disabled.
time_range - (Optional) Specify the time range that applies to the port of the POE. If time range is configured, the power can only be supplied during the period specified by time range. <range_name 32> - Enter the time range name here. This name can be up to 32 characters long. **clear_time_range** - (Optional) Remove the time range.
priority - (Optional) Port priority determines the priority the system attempts to supply the power to port. There are three levels of priority that can be selected, critical, high, and low. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of priority will affect the ordering of supplying power. Whether the disconnect_method is set to deny_low_priority_port, priority of port will be used by the system to manage to supply power to ports. **critical** - Specify that the priority will be set to critical. **high** - Specify that the priority will be set to high. **low** - Specify that the priority will be set to low.
power_limit - (Optional) Configure the per-port power limit. If a port exceeds its power limit, it will be shut down. **class_0** - Specify that the power limit will be set to class 0. **class_1** - Specify that the power limit will be set to class 1. **class_2** - Specify that the power limit will be set to class 2. **class_3** - Specify that the power limit will be set to class 3.
user_define - (Optional) Specify that a user defined per-port power limit will be used. **<value 1000-35000>** - Enter the user defined per-port power limit here. This value must be between m and n.

Restrictions

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

Example

To config PoE port:

```
DES-3200-28P:admin#config poe ports 1-4 state enable priority critical power_li
mit class_1
Command: config poe ports 1-4 state enable priority critical power_limit
class_1

Success.

DES-3200-28P:admin#config poe ports 5 state enable priority critical power_lim
it user_define 1000
Command: config poe ports 5 state enable priority critical power_limit
user_define 1000

Success.

DES-3200-28P:admin#
```

53-3 show poe system

Description

This command is used to display the setting and actual values of the whole PoE system.

Format

show poe system

Parameters

None.

Restrictions

None.

Example

To display PoE system:

```
DES-3200-28P:admin#show poe system
Command: show poe system

PoE System Information
-------------------------------------------------
Power Limit                : 188(Watts)
Power Consumption          : 0(Watts)
Power Remained             : 169(Watts)
Power Disconnection Method : Deny Next Port
Detection Legacy PD        : Disabled




If Power Disconnection Method is set to deny next port, then the system can not
utilize out of its maximum power capacity. The maximum unused watt is 19W.

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

53-4 show poe ports

Description

This command is used to display the setting and actual values of PoE port.

Format

show poe ports {<portlist>}

Parameters

<portlist> - (Optional) Specify a list of ports to be displayed.
If no parameter specified, the system will display the status for all ports.

Restrictions

None.

Example

To display PoE port:

```
DES-3200-28P:admin#show poe ports 1-6
Command: show poe ports 1-6

Port   State     Priority  Power Limit(mW)     Time Range
       Class     Power(mW) Voltage(decivolt)   Current(mA)
       Status
================================================================================
1      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
2      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
3      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
4      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
5      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
6      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Chapter 54 PPPoE Circuit ID Insertions Command List

config pppoe circuit_id_insertion state [enable | disable]
config pppoe circuit_id_insertion ports <portlist> {state [enable | disable] | circuit_id [mac | ip | udf <string 32>]}(1)
show pppoe circuit_id_insertion
show pppoe circuit_id_insertion ports {<portlist>}

54-1 config pppoe circuit_id_insertion state

Description

This command is used to enable or disable PPPoE circuit ID insertion function. When both port and global state are enabled, the system will insert the circuit ID tag to the received PPPoE discover and request packet if the tag is absent, and remove the circuit ID tag from the received PPPoE offer and session confirmation packet. The insert circuit ID contains the following information: Client MAC address, Device ID and Port number. By default, Switch IP address is used as the device ID to encode the circuit ID option.

Format

config pppoe circuit_id_insertion state [enable | disable]

Parameters

enable - Specify to enable the PPPoE circuit ID insertion on the Switch.
disable - Specify to disable the PPPoE circuit ID insertion on the Switch. This is the default.

Restrictions

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

Example

To enable the PPPoE circuit insertion state:

```
DES-3200-28P:admin#config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable

Success.

DES-3200-28P:admin#
```

54-2 config pppoe circuit_id_insertion ports

Description

This command is used to configure port's PPPoE Circuit ID insertion function. When the port's state and the global state are enabled, the system will insert the Circuit ID TAG to the received PPPoE discovery initiation and request packet if the TAG is absent, and remove the Circuit ID TAG from the received PPPoE offer and session confirmation packet.

Format

config pppoe circuit_id_insertion ports <portlist> {state [enable | disable] | circuit_id [mac | ip | udf <string 32>]}(1)

Parameters

<portlist> - Specify a list of ports to be configured.
state - Specify to enable or disable port's PPPoE circuit ID insertion function. The default setting is enable. **enable** - Enable port's PPPoE circuit ID insertion function. **disable** - Disable port's PPPoE circuit ID insertion function.
circuit_id - Configure the device ID part for encoding of the circuit ID option. **mac** - The MAC address of the Switch will be used to encode the circuit ID option. **ip** - The Switch's IP address will be used to encode the circuit ID option. This is the default. **udf** - A user specified string to be used to encode the circuit ID option. **<string 32>** - Enter a string with the maximum length of 32.

Restrictions

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

Example

To enable port 5 PPPoE circuit ID insertion function:

```
DES-3200-28P:admin#config pppoe circuit_id_insertion ports 5 state enable
Command: config pppoe circuit_id_insertion ports 5 state enable

Success.

DES-3200-28P:admin#
```

54-3 show pppoe circuit_id_insertion

Description

This command is used to display PPPoE circuit ID insertion status.

Format

show pppoe circuit_id_insertion

Parameters

None.

Restrictions

None.

Example

To display PPPoE circuit ID insertion status:

```
DES-3200-28P:admin#show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Global PPPoE State: Enabled


DES-3200-28P:admin#
```

54-4 show pppoe circuit_id_insertion ports

Description

This command is used to display Switch's port PPPoE Circuit ID insertion configuration.

Format

show pppoe circuit_id_insertion ports {<portlist>}

Parameters

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

Restrictions

None.

Example

To display port 2-5 PPPoE circuit ID insertion configuration:

```
DES-3200-28P:admin#show pppoe circuit_id_insertion ports  2-5
Command: show pppoe circuit_id_insertion ports 2-5

Port State    Circuit ID
---- -------- ---------------------------------------------
2    Enabled  Switch IP
3    Enabled  Switch IP
4    Enabled  Switch IP
5    Enabled  Switch IP


DES-3200-28P:admin#
```

Chapter 55 Protocol VLAN Command List

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

55-1 create dot1v_protocol_group

Description

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

Format

create dot1v_protocol_group group_id < id> {group_name <name 32>}

Parameters

group_id - The ID of protocol group which is used to identify a set of protocols **<id>** - Enter the group ID used here.
group_name - (Optional) The name of the protocol group. The maximum length is 32 chars. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.

Restrictions

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

Example

To create a protocol group:

```
DES-3200-28P:admin#create dot1v_protocol_group group_id 10 group_name
General_Group
Command: create dot1v_protocol_group group_id 10 group_name General_Group

Success.

DES-3200-28P:admin#
```

55-2 config dot1v_protocol_group add protocol

Description

This command is used to add a protocol to a protocol group. The selection of a protocol can be a pre-defined protocol type or a user defined protocol.

Format

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

Parameters

group_id - The ID of the protocol group which is used to identify a set of protocols. **<id>** - Enter the group ID used here.
group_name - The name of the protocol group. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.
add - Specify that the protocol will be added to the specified group.
delete - Specify that the protocol will be removed from the specified group.
protocol - The protocol value is used to identify a protocol of the frame type specified. **ethernet_2** - Specify that the Ethernet 2 protocol will be used. **ieee802.3_snap** - Specify that the IEEE 802.3 Snap protocol will be used. **ieee802.3_llc** - Specify that the IEEE 802.3 LLC protocol will be used. **<protocol_value>** - Enter the protocol value here.

Restrictions

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

Example

To add a protocol ipv6 to protocol group 10:

```
DES-3200-28P:admin#config dot1v_protocol_group group_id 10 add protocol
ethernet_2 86dd
Command: config dot1v_protocol_group group_id 10 add protocol ethernet_2 86DD


Success.


DES-3200-28P:admin#
```

55-3 delete dot1v_protocol_group

Description

This command is used to delete a protocol group

Format

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

Parameters

group_id - Specify the group ID to be deleted. **<id>** - Enter the group ID used here.
group_name - Specify the name of the group to be deleted. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.
all - Specify that all the protocol group will be deleted.

Restrictions

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

Example

To delete protocol group 100:

```
DES-3200-28P:admin#delete dot1v_protocol_group group_id 100
Command: delete dot1v_protocol_group group_id 100

Success.

DES-3200-28P:admin#
```

55-4 show dot1v_protocol_group

Description

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

Format

show dot1v_protocol_group {[group_id <id> | group_name <name 32>]}

Parameters

group_id - (Optional) Specify the ID of the group to be displayed. **<id>** - Enter the group ID used here.
group_name - (Optional) Specify the name of the protocol group to be displayed. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.
If no group ID is not specified, all the configured protocol groups will be displayed.

Restrictions

None.

Example

To display the protocol group ID 10:

```
DES-3200-28P:admin#show dot1v_protocol_group group_id 10
Command: show dot1v_protocol_group group_id 10

Protocol Group ID Protocol Group Name              Frame Type     Protocol Value
----------------- -------------------------------- -------------- --------------
10                General_Group                    EthernetII     86DD

Total Entries: 1

DES-3200-28P:admin#
```

55-5 config port dot1v

Description

This command is used to assign the VLAN for untagged packets ingress from the port list based on the protocol group configured. This assignment can be removed by using the delete protocol_group option.

When priority is not specified in the command, the port default prority will be the priority for those untagged packets classified by the protocol vlan.

Format

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

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specify that all the ports will be used for this configuration.
add - Specify that the group specified will be added.
protocol_group - Specify that parameters for the group will follow.
group_id - Specify the group ID of the protocol group. **<id>** - Enter the group ID used here.
group_name - Specify the name of the protocol group. **<name 32>** - Enter the name of the group used here. This name can be up to 32 characters long.
vlan - The VLAN that is to be associated with this protocol group on this port. **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
vlanid - Specify the VLAN ID. **<id>** - Enter the VLAN ID used here.
priority - (Optional) Specify the priority to be associated with the packet which has been classified to the specified VLAN by the protocol. **<value 0-7>** - Enter the priority value here. This value must be between 0 and 7.
delete - Specify that the group specified will be deleted.
protocol_group - Specify that parameters for the group will follow.
group_id - Specify the group ID of the protocol group. **<id>** - Enter the group ID used here. **all** - Specify that all the groups will be deleted.

Restrictions

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

Example

The example is to assign VLAN marketing-1 for untaged ipv6 packet ingress from port 3.

To configure the group ID 10 on port 3 to be associated with VLAN marketing-1:

```
DES-3200-28P:admin#config port dot1v ports 3 add protocol_group group_id 10
vlan marketing-1
Command: config port dot1v ports 3 add protocol_group group_id 10 vlan
marketing-1

Success.

DES-3200-28P:admin#
```

55-6 show port dot1v

Description

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

Format

show port dot1v {ports <portlist>}

Parameters

ports - (Optional) Specify a range of ports to be displayed. **<portlist>** - Enter a list of ports used for the configuration here.
If not port is specified, information for all ports will be displayed.

Restrictions

None.

Example

The example display the protocol VLAN information for ports 1:

```
DES-3200-28P:admin#show port dot1v ports 1
Command: show port dot1v ports 1

Port: 1
 Protocol Group ID     VLAN Name                          Protocol Priority
 -------------------   --------------------------------   -----------------
 1                     default                            -
 2                     VLAN2                              -
 3                     VLAN3                              -
 4                     VLAN4                              -

Success.

DES-3200-28P:admin#
```

Chapter 56 QinQ Command List

enable qinq
disable qinq
config qinq inner_tpid <hex 0x1-0xffff>
config qinq ports [<portlist> | all] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1-0xffff> | add_inner_tag [<hex 0x1-0xffff> | disable]}
show qinq
show qinq inner_tpid
show qinq ports {<portlist>}
create vlan_translation ports [<portlist> | all] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}
delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}
show vlan_translation {[ports <portlist> | cvid <vidlist>]}

56-1 enable qinq

Description

This command is used to enable QinQ. When QinQ is enabled, all network port roles will be NNI ports and outer TPID will be set to 0x88A8; all existing static VLANs will run as S-VLAN; all dynamic learned L2 address will be cleared; all dynamic registered VLAN entries will be cleared; and GVRP will be disabled.

To run GVRP on the Switch, the administrator should enable GVRP manually. In QinQ mode, GVRP protocol will employ reserve address 01-80-C2-00-00-0D.

Format

enable qinq

Parameters

None.

Restrictions

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

Example

To enable QinQ:

```
DES-3200-28P:admin#enable qinq
Command: enable qinq

Success.

DES-3200-28P:admin#
```

56-2 disable qinq

Description

This command is used to disable the QinQ. When QinQ is disabled, all dynamic learned L2 addresses will be cleared, all dynamic registered VLAN entries will be cleared, and GVRP will be disabled.

To run GVRP on the Switch, the administrator should enable GVRP manually.

Format

disable qinq

Parameters

None.

Restrictions

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

Example

To disable QinQ:

```
DES-3200-28P:admin#disable qinq
Command: disable qinq

Success.

DES-3200-28P:admin#
```

56-3 config qinq inner_tpid

Description

The command is used to configure the inner TPID of the system. The inner TPID is used to decide if the ingress packet is c-tagged. Inner tag TPID is per system configurable.

Format

config qinq inner_tpid <hex 0x1-0xffff>

Parameters

inner_tpid - Specify the inner-TPID of the system. **<hex 0x1-0xffff>** - Enter the inner-TPID of the system here.

Restrictions

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

Example

To configure the inner TPID in the system to 0x9100:

```
DES-3200-28P:admin#config qinq inner_tpid 0x9100
Command: config qinq inner_tpid 0x9100

Success.

DES-3200-28P:admin#
```

56-4 config qinq ports

Description

This command is used to configure the QinQ port's parameters.

Format

config qinq ports [<portlist> | all] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1-0xffff> | add_inner_tag [<hex 0x1-0xffff> | disable]}

Parameters

ports - Specify a range of ports to configure. **<portlist>** - Enter the list of ports to be configured here. **all** - Specify that all the ports will be used for the configuration.
role - (Optional) Specify the port role in QinQ mode. **uni** - Specify that the port is connecting to the customer network. **nni** - Specify that the port is connecting to the service provider network.
missdrop - (Optional) Specify the state of the miss drop of ports option. **enable** - Specify that the miss drop of ports option will be enabled. **disable** - Specify that the miss drop of ports option will be disabled.
outer_tpid - (Optional) Specify the outer-TPID of a port. **<hex 0x1-0xffff>** - Enter the outer-TPID value used here.
add_inner_tag - (Optional) Specify to add an inner tag for ingress untagged packets. If set, the inner tag will be added for the ingress untagged packets and therefore the packets that egress to the NNI port will be double tagged. If disable, only the s-tag will be added for ingress untagged packets. **<hex 0x1-0xffff>** - Enter the inner tag value used here. **disable** - Specify that the add inner tag option will be disabled.

Restrictions

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

Example

To configure port list 1-4 as NNI port and set the TPID to 0x88A8:

```
DES-3200-28P:admin#config qinq ports 1-4 role nni outer_tpid 0x88A8
Command: config qinq ports 1-4 role nni outer_tpid 0x88A8

Success.

DES-3200-28P:admin#
```

56-5 show qinq

Description

This command is used to display the global QinQ status.

Format

show qinq

Parameters

None.

Restrictions

None.

Example

To display the global QinQ status:

```
DES-3200-28P:admin#show qinq
Command: show qinq

 QinQ Status : Enabled

DES-3200-28P:admin#
```

56-6 show qinq inner_tpid

Description

This command is used to display the inner-TPID of a system.

Format

show qinq inner_tpid

Parameters

None.

Restrictions

None.

Example

To display the inner-TPID of a system:

```
DES-3200-28P:admin#show qinq inner_tpid
Command: show qinq inner_tpid

 Inner TPID: 0x9100


DES-3200-28P:admin#
```

56-7 show qinq ports

Description

This command is used to display the QinQ configuration of the ports.

Format

show qinq ports {<portlist>}

Parameters

ports - Specify a list of ports to be displayed. **<portlist>** - (Optional) Enter the list of ports to be displayed here.

Restrictions

None.

Example

To show the QinQ mode for ports 1-2:

```
DES-3200-28P:admin#show qinq ports 1-2
Command: show qinq ports 1-2


Port ID:    1
-------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x8100
  Add Inner Tag:            Disabled

Port ID:    2
-------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x8100
  Add Inner Tag:            Disabled

DES-3200-28P:admin#
```

56-8 create vlan_translation ports

Description

This command is used to create a VLAN translation rule. This setting will not be effective when the QinQ mode is disabled.

This configuration is only effective for a UNI port. At UNI port, the ingress C-VLAN tagged packets will be translated to S-VLAN tagged packets by adding or replacing according the configured rule. The S-VLAN Tag of egress packets at this port will be recovered to C-VLAN Tag or stripped.

Format

create vlan_translation ports [<portlist> | all] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}

Parameters

ports - Specify a list of ports to be configured. **<portlist>** - Enter the list of ports to be configured here. **all** - Specify that all the ports will be used for the configuration.
add - Specify to add an S-Tag to the packet. **cvid** - Specify the customer VLAN ID used. **<vidlist>** - Enter the customer VLAN ID used here.
replace - Specify to replace the C-Tag with the S-Tag. **cvid** - Specify the customer VLAN ID used. **<vlanid 1-4094>** - Enter the customer VLAN ID used here. **svid** - Specify the service provider VLAN ID used. **<vlanid 1-4094>** - Enter the service provider VLAN ID used here.
priority - (Optional) Specify to assign an 802.1p priority to the S-Tag. If the priority is not specified, the priority of the ports will be set to S-TAG by default. **<priority 0-7>** - Enter the 802.1p S-Tag priority value here. This value must be between 0 and 7.

Restrictions

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

Example

To replace the C-Tag in which the CVID is 20, with the S-Tag and the S-VID is 200 at UNI Port 1:

```
DES-3200-28P:admin#create vlan_translation ports 1 replace cvid 20 svid 200
Command: create vlan_translation ports 1 replace cvid 20 svid 200

Success.

DES-3200-28P:admin#
```

To add S-Tag, when the S-VID is 300, to a packet in which the CVID is 30 at UNI Port 1:

```
DES-3200-28P:admin#create vlan_translation ports 1 add cvid 30 svid 300
Command: create vlan_translation ports 1 add cvid 30 svid 300

Success.

DES-3200-28P:admin#
```

56-9 delete vlan_translation ports

Description

This command is used to delete translation relationships between the C-VLAN and the S-VLAN.

Format

delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}

Parameters

ports - Specify a list of ports to be configured. **<portlist>** - Enter the list of ports to be configured here. **all** - Specify that all the ports will be used for the configuration.
cvid - (Optional) Specify the rules for the specified CVIDs. If the CVID is not specified, all rules configured for the port will be deleted. **<vidlist>** - Enter the CVID value here.

Restrictions

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

Example

To delete a VLAN translation rule on ports 1-4:

```
DES-3200-28P:admin#delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DES-3200-28P:admin#
```

56-10 show vlan_translation

Description

This command is used to display the existing C-VLAN-based VLAN translation rules.

Format

show vlan_translation {[ports <portlist> | cvid <vidlist>]}

Parameters

ports – (Optional) Specify a list of ports to be displayed. **<portlist>** - Enter the list of ports to be displayed here.
cvid - (Optional) Specify the rules for the specified CVIDs. **<vidlist>** - Enter the CVID value used here.

Restrictions

None.

Example

To show C-VLANs based on VLAN translation rules in the system:

```
DES-3200-28P:admin#show vlan_translation
Command: show vlan_translation

Port    CVID       SPVID      Action    Priority
-----   --------   --------   -------   ---------
1       20         200        Replace   -
1       30         300        Add       -

 Total Entries: 2

DES-3200-28P:admin#
```

Chapter 57 Quality of Service (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 per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-1024000>]} max_rate [no_limit | <value 64-1024000>]}
show per_queue bandwidth_control {<portlist>}
config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]
config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr]
show scheduling {<portlist>}
show scheduling_mechanism {<portlist>}
config 802.1p user_priority <priority 0-7> <class_id 0-7>
show 802.1p user_priority
config 802.1p default_priority [<portlist> | all] <priority 0-7>
show 802.1p default_priority {<portlist>}
config 802.1p map {[<portlist> | all]} 1p_color <priority_list> to [green | red | yellow]
show 802.1p map 1p_color {<portlist>}
config dscp trust [<portlist> | all] state [enable | disable]
show dscp trust {<portlist>}
config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63> | dscp_color <dscp_list> to [green | red | yellow]]
show dscp map {<portlist>} [dscp_priority | dscp_dscp | dscp_color] {dscp <dscp_list>}

57-1 config bandwidth_control

Description

This command is used to configure the port bandwidth limit control.

Format

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}

Parameters

<portlist> - Specify a range of ports to be configured.
all – Specify that all the ports will be used for this configuration.
rx_rate - (Optional) Specify the limitation applied to receive data rate. **no_limit** - Indicates there is no limit on receiving bandwidth of the configured ports. An integer value from m to n sets a maximum limit in Kbits/sec. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the command is executed. **<value 64-1024000>** - Enter the receiving data rate here. This value must be between 64 and 1024000.
tx_rate - (Optional) Specify the limitation applied to transmit data rate. **no_limit** - Indicates there is no limit on port tx bandwidth. An integer value from m to n sets a maximum limit in Kbits/sec. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the

command is executed.
<value 64-1024000> - Enter the transmitting data rate here. This value must be between 64 and 1024000.

Restrictions

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

Example

To configure the port bandwidth:

```
DES-3200-28P:admin#config bandwidth_control 1-10 tx_rate 100
Command: config bandwidth_control 1-10 tx_rate 100

 Granularity: RX: 64, TX: 64. Actual Rate: TX: 64.

Success
```

57-2 show bandwidth_control

Description

This command is used to display the port bandwidth configurations.

The bandwidth can also be assigned by the RADIUS server through the authentication process. If RADIUS server has assigned the bandwidth, then the RADIUS-assigned bandwidth will be the effective bandwidth. The authentication with the RADIUS sever can be per port or per user. For per-user authentication, there may be multiple bandwidth control values assigned when there are multiple users attached to this specific port. In this case, the largest assigned bandwidth value will be applied to the effective bandwidth for this specific port. Note that only devices that support MAC-based VLAN can provide per user authentication.

Format

show bandwidth_control {<portlist>}

Parameters

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

Restrictions

None.

Example

To display port bandwidth control table:

```
DES-3200-28P:admin#show bandwidth_control 1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

 Port   RX Rate       TX Rate       Effective RX       Effective TX
        (Kbit/sec)    (Kbit/sec)    (Kbit/sec)         (Kbit/sec)
 -----  ----------    ----------    ----------------   ----------------
 1      No Limit      64            No Limit           64
 2      No Limit      64            No Limit           64
 3      No Limit      64            No Limit           64
 4      No Limit      64            No Limit           64
 5      No Limit      64            No Limit           64
 6      No Limit      64            No Limit           64
 7      No Limit      64            No Limit           64
 8      No Limit      64            No Limit           64
 9      No Limit      64            No Limit           64
 10     No Limit      64            No Limit           64


DES-3200-28P:admin#
```

57-3 config per_queue bandwidth_control

Description

This command is used to configure per port CoS bandwidth control.

Format

config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-1024000>]} max_rate [no_limit | <value 64-1024000>]}

Parameters

ports - (Optional) Specify a range of ports to be configured. **<portlist>** - Enter the list of port used for this configuration here. **all** - For set all ports in the system, you may use “all” parameter. If no parameter is specified, system will set all ports.
<cos_id_list 0-7> - Specify a list of priority queues. The priority queue number is ranged from 0 to 7.
min_rate - (Optional) Specify that one of the parameters below (no_limit or <value m-n) will be applied to the mini-rate at which the above specified class will be allowed to receive packets. **no_limit** - Specify that there will be no limit on the rate of packets received by the above specified class. **<value 64-1024000>** - Specify the packet limit, in Kbps, that the above ports will be allowed to receive. If the specified rate is not multiple of minimum granularity, the rate will be adjusted.
max_rate - (Optional) Specify that one of the parameters below (no_limit or <value m-n >) will be applied to the maximum rate at which the above specified class will be allowed to transmit packets. **no_limit** - Specify that there will be no limit on the rate of packets received by the above specified class. **<value 64-1024000>** - Specify the packet limit, in Kbps, that the above ports will be allowed to

receive. If the specified rate is not multiple of minimum granularity, the rate will be adjusted.

Restrictions

Only Administrator level can issue this command.

Example

To configure the ports 1-10 CoS bandwidth queue 1 min rate to 130 and max rate to 100000:

```
DES-3200-28P:admin#config per_queue bandwidth_control ports 1-10 1 min_rate 130
max_rate 1000
Command: config per_queue bandwidth_control ports 1-10 1 min_rate 130 max_rate
1000

 Granularity: TX: 64. Actual Rate: MIN: 128, MAX: 960.

Success.
```

57-4 show per_queue bandwidth_control

Description

This command is used to display per port CoS bandwidth control settings.

Format

show per_queue bandwidth_control {<portlist>}

Parameters

<portlist> - (Optional) Specify a range of ports to be displayed.
If no parameter is specified, system will display all ports CoS bandwidth configurations.

Restrictions

None.

Example

Display per port CoS bandwidth control table:

```
DES-3200-28P:admin#show per_queue bandwidth_control 10
Command: show per_queue bandwidth_control 10

Queue Bandwidth Control Table On Port: 10

Queue     Min Rate(Kbit/sec)     Max Rate(Kbit/sec)
0         640                    No Limit
1         640                    No Limit
2         640                    No Limit
3         640                    No Limit
4         No Limit               No Limit
5         No Limit               No Limit
6         No Limit               No Limit
7         No Limit               No Limit

DES-3200-28P:admin#
```

57-5 config scheduling

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]

Parameters

ports - Specify a range of ports to be configured. **<portlist>** - Enter the list of port used for this configuration here.
<class_id 0-7> - This specifies the 8 hardware priority queues which the config scheduling command will apply to. The four hardware priority queues are identified by number from 0 to 7 with the 0 queue being the lowest priority.
strict - The queue will operate in strict mode.
weight - Specify the weights for weighted round robin. A value between 0 and n can be specified. **<value 1-127>** - Enter the weights for weighted round robin value here. This value must be between 1 and 127.

Restrictions

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

Example

To configure the traffic scheduling CoS queue 1 to weight 25 on port 10:

```
DES-3200-28P:admin#config scheduling ports 10 1 weight 25
Command: config scheduling ports 10 1 weight 25

Success.

DES-3200-28P:admin#
```

57-6 config scheduling_mechanism

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr]

Parameters

ports - (Optional) Specify a range of ports to be configured. **<portlist>** - Enter the list of port used for this configuration here. **all** - For set all ports in the system, you may use "all" parameter. If no parameter is specified, system will set all ports.
strict - All queues operate in strict mode.
wrr - Each queue operates based on its setting.

Restrictions

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

Example

To configure the traffic scheduling mechanism for each CoS queue:

```
DES-3200-28P:admin#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DES-3200-28P:admin#
```

To configure the traffic scheduling mechanism for CoS queue on port 1:

```
DES-3200-28P:admin#config scheduling_mechanism ports 1 strict
Command: config scheduling_mechanism ports 1 strict

Success.

DES-3200-28P:admin#
```

57-7 show scheduling

Description

This command is used to display the current traffic scheduling parameters.

Format

show scheduling {<portlist>}

Parameters

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

Restrictions

None.

Example

To display the traffic scheduling parameters for each CoS queue on port 1(take eight hardware priority queues for example):

```
DES-3200-28P:admin#show scheduling 1
Command: show scheduling 1


QOS Output Scheduling On Port: 1
Class ID  Weight
--------  ------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8


DES-3200-28P:admin#
```

57-8 show scheduling_mechanism

Description

This command is used to show the traffic scheduling mechanism.

Format

show scheduling_mechanism {<portlist>}

Parameters

<portlist> - (Optional) Specify a range of ports to be displayed. If no parameter specified, system will display all ports scheduling mechanism configurations.

Restrictions

None.

Example

To show scheduling mechanism:

```
DES-3200-28P:admin#show scheduling_mechanism
Command: show scheduling_mechanism

Port    Mode
-----   ------
1       Strict
2       Strict
3       Strict
4       Strict
5       Strict
6       Strict
7       Strict
8       Strict
9       Strict
10      Strict
11      Strict
12      Strict
13      Strict
14      Strict
15      Strict
16      Strict
17      Strict
18      Strict
19      Strict
20      Strict
21      Strict
22      Strict
23      Strict
24      Strict
25      Strict
26      Strict
27      Strict
28      Strict


DES-3200-28P:admin#
```

57-9 config 802.1p user_priority

Description

This command is used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the Switch.

Format

config 802.1p user_priority <priority 0-7> <class_id 0-7>

Parameters

<priority 0-7> - The 802.1p user priority you want to associate with the <class_id> (the number of the hardware queue) with.
<class_id 0-7> - The number of the Switch's hardware priority queue. The switch has 8 hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority).

Restrictions

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

Example

To configure the 802.1p user priority:

```
DES-3200-28P:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-3200-28P:admin#
```

57-10 show 802.1p user_priority

Description

This command is used to display 802.1p user priority for ports.

Format

show 802.1p user_priority

Parameters

None.

Restrictions

None.

Example

To display the 802.1p user priority:

```
DES-3200-28P:admin#show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic:
Priority-0  ->  <Class-2>
Priority-1  ->  <Class-0>
Priority-2  ->  <Class-1>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-4>
Priority-5  ->  <Class-5>
Priority-6  ->  <Class-6>
Priority-7  ->  <Class-7>

DES-3200-28P:admin#
```

57-11 config 802.1p default_priority

Description

This command is used to configure the 802.1p default priority settings on the Switch. If an untagged packet is received by the Switch, the priority configured with this command will be written to the packet's priority field.

Format

config 802.1p default_priority [<portlist> | all] <priority 0-7>

Parameters

<portlist> - This specifies a range of ports for which the default priority is to be configured. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The port list is specified by listing the beginning port number on the Switch, separated by a colon. Then highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash.
all - Specify that the command apply to all ports on the Switch.
<priority 0-7> - The priority value (0 to 7) assigned to untagged packets received by the Switch or a range of ports on the Switch.

Restrictions

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

Example

To configure the 802.1p default priority settings on the Switch:

```
DES-3200-28P:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3200-28P:admin#
```

57-12 show 802.1p default_priority

Description

This command is used to display the current configured default priority settings on the Switch.

The default priority can also be assigned by the RADIUS server through the authentication process. The authentication with the RADIUS sever can be per port or port user. For per port authentication, the priority assigned by RADIUS server will be the effective port default priority. For per user authentication, the priority assigned by RADIUS will not be the effective port default priority whereas it will become the priority associated with MAC address. Note that only devices supporting MAC-based VLAN can provide per user authentication.

Format

show 802.1p default_priority {<portlist>}

Parameters

<portlist> - (Optional) Specify a range of ports to be displayed.
If no parameter is specified, all ports for 802.1p default priority will be displayed.

Restrictions

None.

Example

To display 802.1p default priority:

```
DES-3200-28P:admin#show 802.1p default_priority  1-10
Command: show 802.1p default_priority 1-10

Port       Priority      Effective Priority
----       -----------   ------------------
1          5             5
2          5             5
3          5             5
4          5             5
5          5             5
6          5             5
7          5             5
8          5             5
9          5             5
10         5             5

DES-3200-28P:admin#
```

57-13 config dscp trust

Description

This command is used to configure the state of DSCP trust per port. When DSCP is not trusted, 802.1p is trusted.

Format

config dscp trust [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter the list of port used for this configuration.
all - Specify that the command apply to all ports on the Switch.
state - Enable or disable to trust DSCP. By default, DSCP trust is disabled. **enable** - Specify that the DSCP trust state will be enabled. **disable** - Specify that the DSCP trust state will be disabled.

Restrictions

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

Example

Enable DSCP trust on ports 1-8.

```
DES-3200-28P:admin#config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable

Success.

DES-3200-28P:admin#
```

57-14 config 802.1p map

Description

This command is used to configure the mapping of 802.1p to the packet's initial color. The mapping of 802.1p to a color is used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is 1p-trusted.

Format

config 802.1p map {[<portlist> | all]} 1p_color <priority_list> to [green | red | yellow]

Parameters

<portlist> - (Optional) Enter the list of port used for this configuration.
all - (Optional) Specify that the command apply to all ports on the Switch.
1p_color - The list of source priority for imcoming packets. **<priority_list>** - Specify the list of source priority for imcoming packets.
to - The mapped color for a packet.

green - Specify green as the mapped color.
red - Specify red as the mapped color.
yellow - Specify yellow as the mapped color.

Restrictions

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

Example

If a product supports per-port 802.1p mapping configuration, configure the mapping of 802.1p priority 1 to red on ports 1-8.

```
DES-3200-28P:admin#config 802.1p map 1-8 1p_color 1 to red
Command: config 802.1p map 1-8 1p_color 1 to red

Success.

DES-3200-28P:admin#
```

57-15 show 802.1p map 1p_color

Description

This command is used to display the 802.1p to color mapping.

Format

show 802.1p map 1p_color {<portlist>}

Parameters

<portlist> - (Optional) Specify a list of ports.

Restrictions

None.

Example

To show the 802.1p color mapping on port 1:

```
DES-3200-28P:admin#show 802.1p map 1p_color 1
Command: show 802.1p map 1p_color 1

802.1p to Color Mapping:
-------------------------------------------------------------
Port 0      1      2      3      4      5      6      7
---- ------ ------ ------ ------ ------ ------ ------ ------
1    Green  Green  Green  Green  Green  Green  Green  Green

DES-3200-28P:admin#
```

57-16 show dscp trust

Description

This command is used to display DSCP trust state for the specified ports on the Switch.

Format

show dscp trust {<portlist>}

Parameters

<portlist> - (Optional) A range of ports to display.
If not specify the port, all ports for DSCP trust status on the Switch will be displayed.

Restrictions

None.

Example

Display DSCP trust status on ports 1-8.

```
DES-3200-28P:admin#show dscp trust 1-8
Command: show dscp trust 1-8

Port DSCP-Trust
---- ----------
1    Disabled
2    Disabled
3    Disabled
4    Disabled
5    Disabled
6    Disabled
7    Disabled
8    Disabled

DES-3200-28P:admin#
```

57-17 config dscp map

Description

This command is used to configure DSCP mapping. The mapping of DSCP to priority will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The mapping of DSCP to color will be used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is DSCP-trusted.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

These DSCP mapping will take effect at the same time when IP packet ingress from a DSCP-trusted port.

Format

config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63> | dscp_color <dscp_list> to [green | red | yellow]]

Parameters

<portlist> - Enter the list of port used for this configuration here. **all** - Specify that all the ports will be included in this configuration.
dscp_priority - Specify a list of DSCP value to be mapped to a specific priority. **<dscp_list>** - Enter the DSCP priority list here. **to** - Specify that the above or following parameter will be mapped to the previously mentioned parameter. **<priority 0-7>** - Specify the result priority of mapping.
dscp_dscp - Specify a list of DSCP value to be mapped to a specific DSCP. **<dscp_list>** - Enter the DSCP to DSCP list here. **to** - Specify that the above or following parameter will be mapped to the previously mentioned parameter. **<dscp 0-63>** - Specify the result DSCP of mapping.
dscp_color - Specify a list of DSCP value to be mapped to a specific color. **<dscp_list>** - Enter the DSCP to color list here. **to** - Specify that the above or following parameter will be mapped to the previously mentioned parameter. **green** - Specify the result color of mapping to be green. **red** - Specify the result color of mapping to be red. **yellow** - Specify the result color of mapping to be yellow.

Restrictions

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

Example

To configure the mapping of the DSCP priority to priority 1:

```
DES-3200-28P:admin#config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

DES-3200-28P:admin#
```

To configure the global mapping of the DSCP priority to priority 1:

```
DES-3200-28P:admin#config dscp map dscp_priority 1 to 1
Command: config dscp map dscp_priority 1 to 1

Success.

DES-3200-28P:admin#
```

57-18 show dscp map

Description

This command is used to show DSCP trusted port list and mapped color, priority and DSCP.

Format

show dscp map {<portlist>} [dscp_priority | dscp_dscp | dscp_color] {dscp <dscp_list>}

Parameters

<portlist> - (Optional) A range of ports to show. If no parameter is specified, all ports' dscp mapping will be displayed.
dscp_priotity - Specify a list of DSCP value to be mapped to a specific priority.
dscp_dscp - Specify a list of DSCP value to be mapped to a specific DSCP.
dscp_color - Specify a list of DSCP value to be mapped to a specific color.
dscp - (Optional) This specifies DSCP value that will be mapped. **<dscp_list>** - Enter the DSCP list here.

Restrictions

None.

Example

In case of project support per port configure, show DSCP map configuration on port 1.

```
DES-3200-28P:admin#show dscp map 1 dscp_dscp
Command: show dscp map 1 dscp_dscp

DSCP to DSCP Mapping:
-------------------------------------------------------------
Port 1     |   0    1    2    3    4    5    6    7    8    9
-----------+-------------------------------------------------
         0 |   0    1    2    3    4    5    6    7    8    9
         1 |  10   11   12   13   14   15   16   17   18   19
         2 |  20   21   22   23   24   25   26   27   28   29
         3 |  30   31   32   33   34   35   36   37   38   39
         4 |  40   41   42   43   44   45   46   47   48   49
         5 |  50   51   52   53   54   55   56   57   58   59
         6 |  60   61   62   63
-------------------------------------------------------------

DES-3200-28P:admin#
```

Chapter 58 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

58-1 config safeguard_engine

Description

This command is used to configure the CPU protection control for the system.

Format

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

Parameters

state - (Optional) Specify to configure CPU protection state to enable or disable. **enable** - Specify that CPU protection will be enabled. **disable** - Specify that CPU protection will be enabled.
utilization - (Optional) Specify to configure the CPU protection 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. **<20-100>** - Enter the utilization rising value here. This value must be between 20 and 100. **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. **<20-100>** - Enter the utilization falling value here. This value must be between 20 and 100.
trap_log - (Optional) Configure the state of CPU protection related trap/log mechanism to enable or disable. If set to enable, trap and log will be active while cpu protection current mode changed.If set to disable, current mode change will not trigger trap and log events. **enable** - Specify that the CPU protection trap or log mechanism will be enabled. **disable** - Specify that the CPU protection trap or log mechanism will be disabled.
mode - (Optional) determine the controlling method of broadcast traffic. Here are two modes (strict and fuzzy). **strict** - In strict mode, the Switch will stop receiving all 'IP broadcast' packets, packets from the untrusted IP address and reduce the bandwidth of 'ARP not to me' packets (the protocol address of the target in ARP packet is the Switch itself) to the Switch. That means that no matter what the reasons are that cause high CPU utilization (may not be caused by an ARP storm), the Switch reluctantly processes the specified traffic, mentioned previously in the Exhausted mode. **fuzzy** - In fuzzy mode, the Switch will adjust the bandwidth dynamically depending on some reasonable algorithm.

Restrictions

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

Example

To configure CPU protection:

```
DES-3200-28P:admin#config safeguard_engine state enable utilization rising 50
falling 30 trap_log enable
Command: config safeguard_engine state enable utilization rising 50 falling 30
trap_log enable


Success.


DES-3200-28P:admin#
```

58-2 show safeguard_engine

Description

This command is used to show safeguard engine information.

Format

show safeguard_engine

Parameters

None.

Restrictions

None.

Example

To show safeguard_engine information:

```
DES-3200-28P:admin#show safeguard_engine
Command: show safeguard_engine



Safeguard Engine State          :  Disabled
Safeguard Engine Current Status :  Normal Mode
==================================================
CPU Utilization Information:
Rising Threshold  :  30%
Falling Threshold :  20%
Trap/Log State    :  Disabled
Mode              :  Fuzzy

DES-3200-28P:admin#
```

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

Chapter 59 Secure Shell (SSH) Command List

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5| SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm
config ssh authmode [password | publickey | hostbased] [enable | disable]
show ssh authmode
config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>] | password | publickey]
show ssh user authmode
config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}
enable ssh
disable ssh
show ssh server

59-1 config ssh algorithm

Description

This command is used to configure SSH service algorithm.

Format

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5| SHA1 | RSA | DSA] [enable | disable]

Parameters

3DES - The "3DES" cipher is three-key triple-DES (encrypt-decrypt-encrypt), where the first 8 bytes of the key are used for the first encryption, the next 8 bytes for the decryption, and the following 8 bytes for the final encryption.
AES (128,192,256) - Advanced Encryption Standard.
arcfour - RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely-used software stream cipher.
blowfish - Blowfish is a keyed, symmetric block cipher.
cast128 - CAST-128 is a 12- or 16-round feistel network with a 64-bit block size and a key size of between 40 to 128 bits.
twofish (128,192,256) - Twofish has a 128-bit block size, a key size ranging from 128 to 256 bits.
MD5 - Message-Digest Algorithm 5.
SHA1 - Secure Hash Algorithm.
RSA - RSA encryption algorithm is a non-symmetric encryption algorithm.
DSS - Digital Signature Standard.
enable - Enabled the algorithm.
disable - Disables the algorithm.

Restrictions

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

Example

To enable SSH server public key algorithm:

```
DES-3200-28P:admin#config ssh algorithm DSA enable
Command: config ssh algorithm DSA enable

Success.

DES-3200-28P:admin#
```

59-2 show ssh algorithm

Description

This command is used to show the SSH service algorithm.

Format

show ssh algorithm

Parameters

None.

Restrictions

None.

Example

To show server algorithm:

```
DES-3200-28P:admin#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
--------------------------
3DES       : Enabled
AES128     : Enabled
AES192     : Enabled
AES256     : Enabled
Arcfour    : Enabled
Blowfish   : Enabled
Cast128    : Enabled
Twofish128 : Enabled
Twofish192 : Enabled
Twofish256 : Enabled

Data Integrity Algorithm
--------------------------
MD5        : Enabled
SHA1       : Enabled

Public Key Algorithm
--------------------------
RSA        : Enabled
DSA        : Enabled

DES-3200-28P:admin#
```

59-3 config ssh authmode

Description

This command is used to configure user authentication method for SSH.

Format

config ssh authmode [password | publickey | hostbased] [enable | disable]

Parameters

password - Specify user authentication method. **publickey** - Specify user authentication method. **hostbased** - Specify user authentication method.
enable - Enable user authentication method. **disable** - Disable user authentication method.

Restrictions

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

Example

To configure user authentication method:

```
DES-3200-28P:admin#config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DES-3200-28P:admin#
```

59-4 show ssh authmode

Description

This command is used to show the user authentication method.

Format

show ssh authmode

Parameters

None.

Restrictions

None.

Example

To show user authentication method:

```
DES-3200-28P:admin#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password    : Enabled
Public Key  : Enabled
Host-based  : Enabled


DES-3200-28P:admin#
```

59-5 config ssh user

Description

This command is used to update user information for SSH configuration.

Format

config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>] | password | publickey]

Parameters

<username 15> - Enter the user name used here. This name can be up to 15 characters long.
automode - Specify user authentication method.
hostbased - Specify as host-based method.
hostname - Specify host domain name.
<domain_name 32> - Enter the domain name here. This name can be up to 32 characters long.
hostname_IP - Specify host domain name and IP address.
<domain_name 32> - Specify host name if configuring Host-based method.
password - Specify user authentication method.
publickey - Specify user authentication method.

Restrictions

Only Administrator-level users can issue this command.

Example

To update user “test” authentication method:

```
DES-3200-28P:admin#config ssh user test authmode publickey
Command: config ssh user test authmode publickey

Success.

DES-3200-28P:admin#
```

59-6 show ssh user

Description

This command is used to show the SSH user information.

Format

show ssh user authmode

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show user information about SSH configuration:

```
DES-3200-28P:admin#show ssh user authmode
Command: show ssh user authmode

Current Accounts
Username          AuthMode             HostName            HostIP
------------  -------------        ------------      -------------
test              Public Key
alpha             Host-based           alpha-local        172.18.61.180
beta              Host-based           beta-local          3000::105
Total Entries : 3

DES-3200-28P:admin#
```

59-7 config ssh server

Description

This command is used to configure the SSH server general information.

Format

config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}

Parameters

maxsession - (Optional) Specify SSH server maximum session at the same time, maximum 8 sessions. **<int 1-8>** - Enter the maximum session value here. This value must be between 1 and 8.
contimeout - (Optional) Specify SSH server connection time-out, in the unit of second. **<sec 120-600>** - Enter the connection time-out value here. This value must be between 120 and 600 seconds.
authfail - (Optional) Specify user maximum fail attempts. **<int 2-20>** - Enter the user maximum fail attempts value here. This value must be between 2 and 20.
rekey - (Optional) Specify time to re-generate session key. There are 10 minutes, 30 minutes, 60 minutes and never for the selection, which the never means do NOT re- generate session key **10min** - Specify that the re-generate session key time will be 10 minutes. **30min** - Specify that the re-generate session key time will be 30 minutes. **60min** - Specify that the re-generate session key time will be 60 minutes. **never** - Specify that the re-generate session key time will be set to never.
port - (Optional) Specify the TCP port used to communication between SSH client and server. The default value is 22. **<tcp_port_number 1-65535>** - Enter the TCP port number here. This value must be between 1 and 65535.

Restrictions

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

Example

To configure SSH server maximum session number is 3:

```
DES-3200-28P:admin#config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DES-3200-28P:admin#
```

59-8 enable ssh

Description

This command is used to enable SSH server services.

Format

enable ssh

Parameters

None.

Restrictions

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

Example

To enable SSH server:

```
DES-3200-28P:admin#enable ssh
Command: enable ssh

Success.

DES-3200-28P:admin#
```

59-9 disable ssh

Description

This command is used to disable SSH server services.

Format

disable ssh

Parameters

None.

Restrictions

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

Example

To disable the SSH server services:

```
DES-3200-28P:admin#disable ssh
Command: disable ssh

Success.

DES-3200-28P:admin#
```

59-10 show ssh server

Description

This command is used to show the SSH server general information.

Format

show ssh server

Parameters

None.

Restrictions

None.

Example

To show SSH server:

```
DES-3200-28P:admin#show ssh server
Command: show ssh server

The SSH Server Configuration
Maximum Session              : 8
Connection Timeout           : 120
Authentication Fail Attempts : 2
Rekey Timeout                : Never
TCP Port Number              : 22


DES-3200-28P:admin#
```

Chapter 60 Secure Sockets Layer (SSL) Command List

download ssl certificate {<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>}
enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
show ssl {certificate}
show ssl cachetimeout
config ssl cachetimeout <value 60-86400>

60-1 download ssl certificate

Description

This command is used to download the certificate to the device according to the certificate level. The user can download the specified certificate to the device which must, according to desired key exchange algorithm. For RSA key exchange, the user must download RSA type certificate and for DHS_DSS is using the DSA certificate for key exchange.

Format

download ssl certificate {<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>}

Parameters

<ipaddr> - (Optional) Enter the TFTP server IP address used for this configuration here.
certfilename - (Optional) Specify the desired certificate file name. **<path_filename 64>** - Certificate file path respect to tftp server root path, and input characters max to 64 octets.
keyfilename - (Optional) Specify the private key file name which accompany with the certificate. **<path_filename 64>** - Private key file path respect to tftp server root path, and input characters max to 64 octets.

Restrictions

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

Example

To download certificate from TFTP server:

```
DES-3200-28P:admin#download ssl certificate 10.55.47.1 certfilename cert.der
keyfilename pkey.der
Command: download ssl certificate 10.55.47.1 certfilename cert.der keyfilename
pkey.der

Success.

DES-3200-28P:admin#
```

60-2 enable ssl

Description

This command is used to enable SSL status and it's ciphersuites. Using "enable ssl" command will enable SSL feature which means enable SSLv3 and TLSv1. For each ciphersuites, user must specify it by this command.

Format

enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

Parameters

ciphersuite - (Optional) Specify the cipher suite combination used for this configuration.
- **RSA_with_RC4_128_MD5** - Indicate RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - Indicate RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - Indicate DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - Indicate RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

Restrictions

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

Example

To enable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DES-3200-28P:admin#enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DES-3200-28P:admin#
```

To enable SSL:

```
DES-3200-28P:admin#enable ssl
Command: enable ssl

Success.

DES-3200-28P:admin#
```

Note: Web will be disabled when SSL is enabled.

60-3 disable ssl

Description

This command is used to disable SSL feature and supported ciphercuites. Using “disable ssl” command will disable SSL feature and for each ciphersuites status user must specified it by this command.

Format

disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

Parameters

ciphersuite - (Optional) Specify the cipher suite combination used for this configuration.
- **RSA_with_RC4_128_MD5** - Indicate RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - Indicate RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - Indicate DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - Indicate RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

Restrictions

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

Example

To disable SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DES-3200-28P:admin#disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DES-3200-28P:admin#
```

To disable SSL:

```
DES-3200-28P:admin#disable ssl
Command: disable ssl

Success.

DES-3200-28P:admin#
```

60-4 show ssl

Description

This command is used to display the certificate status. User must download specified certificate type according to desired key exchange algorithm. The options may be no certificate, RSA type or DSA type certificate

Format

show ssl {certificate}

Parameters

certificate – (Optional) Specify that the SSL certificate will be displayed.

Restrictions

None.

Example

To show SSL:

```
DES-3200-28P:admin#show ssl
Commands: show ssl

SSL Status                                      Enabled

 RSA_WITH_RC4_128_MD5                  0x0004  Enabled
 RSA_WITH_3DES_EDE_CBC_SHA             0x000A  Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA         0x0013  Enabled
 RSA_EXPORT_WITH_RC4_40_MD5            0x0003  Enabled

DES-3200-28P:admin#
```

To show certificate:

```
DES-3200-28P:admin#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DES-3200-28P:admin#
```

60-5 show ssl cachetimeout

Description

This command is used to show cahce timeout value which is designed for dlktimer library to remove the session id after expired. In order to support the resume session feature, the SSL library keep the session id in web server, and invoking the dlktimer library to remove this session id by cache timeout value.

Format

show ssl cachetimeout

Parameters

None.

Restrictions

None.

Example

To show SSL cache timeout:

```
DES-3200-28P:admin#show ssl cachetimeout
Commands: show ssl cachetimeout

Cache timeout is 600 second(s)

DES-3200-28P:admin#
```

60-6 config ssl cachetimeout

Description

This command is used to configure cahce timeout value which is designed for dlktimer library to remove the session id after expired. In order to support the resume session feature, the SSL library keep the session id in web server, and invoking the dlktimer library to remove this session id by cache timeout value. The unit of argument's value is second and it's boundary is between 60 (1 minute) and 86400 (24 hours). Default value is 600 seconds.

Format

config ssl cachetimeout <value 60-86400>

Parameters

timeout - Specify the SSL cache timeout value attributes. **<value 60-86400>** - Enter the timeout value here. This value must be between 60 and 86400.

Restrictions

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

Example

To configure the SSL cache timeout value to 60:

```
DES-3200-28P:admin#config ssl cachetimeout 60
Commands: config ssl cachetimeout 60

Success.

DES-3200-28P:admin#
```

Chapter 61 Show Technical Support Command List

show tech_support
upload tech_support_toTFTP {<ipaddr> <path_filename 64>}

61-1 show tech_support

Description

This command is especially used by the technical support personnel to dump the device overall operation information.

- Basic System information
- System log
- Running configuration
- Layer 1 information
- Layer 2 information
- Layer 3 information
- Application
- OS status
- Controller's status

This command can be interrupted by Ctrl - C or ESC when it is executing.

Format

show tech_support

Parameters

None.

Restrictions

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

Example

To show the information of technique's support:

```
DES-3200-28P:admin#show tech_support
Command: show tech_support

#-------------------------------------------------------------------------
#                       DES-3200-28P Fast Ethernet Switch
#                         Technical Support Information
#
#                            Firmware: Build 4.03.004
#          Copyright(C) 2011  D-Link Corporation. All rights reserved.
#-------------------------------------------------------------------------

********************   Basic System Information   ********************

[SYS 2000-1-1 02:35:27]
Boot Time           : 1 Jan 2000  00:00:14
RTC Time            : 2000/01/01 02:35:27
Boot PROM Version   : Build 4.00.001
Firmware Version    : Build 4.03.004
Hardware Version    : C1
MAC Address         : 00-01-02-03-04-00
[ERROR_LOG 2000-1-1 02:35:27]

*************************************************************************

# debug log: 1
# firmware version: 4.03.T003
# level: fatal
# clock: 37930 ms
# time : 2000-02-13 06:15:28

====================== SOFTWARE FATAL ERROR ======================

SDK ERROR: Assertion failed: (SOC_REG_IS_VALID(unit, reg)) at reg.c:1209
Current TASK : ST_hCFG
```

61-2 upload tech_support_toTFTP

Description

This command is used to upload the information of technique's support to TFTP server.

- Basic System information
- System log
- Running configuration
- Layer 1 information
- Layer 2 information
- Layer 3 information
- Application
- OS status
- Controller's status

This command can be interrupted by Ctrl - C or ESC when it is executing.

Format

upload tech_support_toTFTP {<ipaddr> <path_filename 64>}

Parameters

<ipaddr> - (Optional) Specify the IP address of TFTP server.
<path_filename 64> - Specify the file name to store the information of technique's support in TFTP server. The max size of the file name is 64.

Restrictions

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

Example

To upload the information of technique's support:

```
DES-3200-28P:admin#upload tech_support_toTFTP 10.0.0.66 tech_report.txt
Command: upload tech_support_toTFTP 10.0.0.66 tech_report.txt

 Connecting to server.................. Done.
 Upload techsupport file............... Done.

 Success.

DES-3200-28P:admin#
```

Chapter 62 Simple Mail Transfer Protocol (SMTP) Command List

enable smtp
disable smtp
config smtp {server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | [add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8>]}(1)
show smtp
smtp send_testmsg

62-1 enable smtp

Description

This command is used to enable the SMTP status.

Format

enable smtp

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SMTP status:

```
DES-3200-28P:admin#enable smtp
Command: enable smtp

Success.

DES-3200-28P:admin#
```

62-2 disable smtp

Description

This command is used to disable SMTP status.

Format

disable smtp

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SMTP status:

```
DES-3200-28P:admin#disable smtp
Command: disable smtp

Success.

DES-3200-28P:admin#
```

62-3 config smtp

Description

This command is used to configure SMTP settings.

Format

config smtp {server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | [add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8>]}(1)

Parameters

server - Specify the SMTP server IP address. **<ipaddr>** - Enter the SMTP server IP address
server_port - Specify the SMTP server port. **<tcp_port_number 1-65535>** - Enter the port number between 1 and 65535.
self_mail_addr - Specify the sender's mail address. **<mail_addr 64>** - Enter the mail address with maximum of 64 characters.
add mail_receiver – Specify to add mail receiver's address. **<mail_addr 64>** - Enter the mail address with maximum of 64 characters.
delete mail_receiver – Specify to delete mail receiver's address. **<index 1-8>** - Enter the index number.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure a SMTP server IP address:

```
DES-3200-28P:admin#config smtp server 172.18.208.9
Command: config smtp server 172.18.208.9

Success.

DES-3200-28P:admin#
```

To configure an SMTP server port:

```
DES-3200-28P:admin#config smtp server_port 25
Command: config smtp server_port 25

Success.

DES-3200-28P:admin#
```

To configure a mail source address:

```
DES-3200-28P:admin#config smtp self_mail_addr mail@dlink.com
Command: config smtp self_mail_addr mail@dlink.com

Success.

DES-3200-28P:admin#
```

To add a mail destination address:

```
DES-3200-28P:admin#config smtp add mail_receiver receiver@dlink.com
Command: config smtp add mail_receiver receiver@dlink.com

Success.

DES-3200-28P:admin#
```

To delete a mail destination address:

```
DES-3200-28P:admin#config smtp delete mail_receiver 1
Command: config smtp delete mail_receiver 1

Success.

DES-3200-28P:admin#
```

62-4 show smtp

Description

This command is display the current SMTP information.

Format

show smtp

Parameters

None.

Restrictions

None.

Example

To display the current SMTP information:

```
DES-3200-28P:admin#show smtp
Command: show smtp

SMTP Status             : Disabled
SMTP Server Address     : 172.18.208.9
SMTP Server Port        : 25
Self Mail Address       : mail@dlink.com

Index    Mail Receiver Address
-----    ------------------------------------------------------------------------
1        receiver@dlink.com
2
3
4
5
6
7
8


DES-3200-28P:admin#
```

62-5 smtp send_testmsg

Description

This command is used to test whether the SMTP server can be reached.

Format

smtp send_testmsg

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To test whether the SMTP server can be reached:

```
DES-3200-28P:admin#smtp send_testmsg
Command: smtp send_testmsg

Subject:e-mail heading
Content:e-mail content

Sending mail, please wait...

Success.

DES-3200-28P:admin#
```

Chapter 63 Simple Network Management Protocol (SNMP) Command List

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community <community_string 32>
show snmp community {<community_string 32>}
create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user <username 32>
show snmp user
create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group <groupname 32>
show snmp groups
create snmp view <view_name 32> <oid> view_type [included | excluded]
delete snmp view <view_name 32> [all | <oid>]
show snmp view {<view_name 32>}
create snmp host <ipaddr>[v1|v2c|v3[noauth_nopriv|auth_nopriv|auth_priv]]<auth_string32>
delete snmp host <ipaddr>
show snmp host {<ipaddr>}
config snmp engineID <snmp_engineID 10-64>
show snmp engineID
enable snmp
disable snmp
config snmp system_name {<sw_name>}
config snmp system_location {<sw_location>}
config snmp system_contact {<sw_contact>}
enable snmp traps
disable snmp traps
enable snmp authenticate_traps
disable snmp authenticate_traps
enable snmp linkchange_traps
disable snmp linkchange_traps
config snmp linkchange_traps ports [all | <portlist>] [enable | disable]
config snmp coldstart_traps [enable | disable]
config snmp warmstart_traps [enable | disable]
show snmp traps {linkchange_traps {ports <portlist>}}
config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]} (1)
show rmon

63-1 create snmp community

Description

This command is used to create an SNMP community string.

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

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

A MIB view, which defines the subset of all MIB objects accessible to the given community.

Read and write or read-only permission for the MIB objects accessible to the community.

Format

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

Parameters

community - An alphanumeric string of up to 32 characters used to authentication of users wanting access to the Switch's SNMP agent. **<community_string>** - Enter the community string value here.
view_name - Specify to view a MIB name. **<view_name 32>** - Enter the MIB view name here. This name can be up to 32 characters long.
readonly - Allows the user using the above community string to have read only access to the Switch's SNMP agent. **readwrite** - Allows the user using the above community string to have read and write access to the Switch's SNMP agent. The default read only community string is public. The default read write community string is private.

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DES-3200-28P:admin#create snmp community System view CommunityView read_only
Command: create snmp community System view CommunityView read_only

Success.

DES-3200-28P:admin#
```

63-2 delete snmp community

Description

This command is used to delete an SNMP community string.

Format

delete snmp community <community_string 32>

Parameters

community - Community string will be deleted. **<community_string 32>** - Enter the community string value here. This value can be up to 32 characters long.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a SNMP community “System”:

```
DES-3200-28P:admin#delete snmp community System
Command: delete snmp community System

Success.

DES-3200-28P:admin#
```

63-3 show snmp community

Description

This command is used to display the community string configurations.

Format

show snmp community <community_string 32>

Parameters

<community_string 32> - (Optional) Specify the Community string.
If not specify community string , all community string information will be displayed.

Restrictions

None.

Example

To display SNMP community:

```
DES-3200-28P:admin#show snmp community
Command: show snmp community

SNMP Community Table
Community Name                          View Name           Access Right
------------------------------  ----------------------  ------------
private                                  CommunityView      read_write
public                                   CommunityView      read_only

Total Entries : 2

DES-3200-28P:admin#
```

63-4 create snmp user

Description

This command is used to create a new user to an SNMP group originated by this command.

Format

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

Parameters

<user_name 32> - The name of the user on the host that connects to the agent. The range is 1 to 32.
<groupname 32> - The name of the group to which the user is associated. The range is 1 to 32.
encrypted - (Optional) Specify whether the password appears in encrypted format.
by_password - (Optional) Indicate input password for authentication and privacy. **auth** - Initiates an authentication level setting session. The options are md5 and sha. **md5** - The HMAC-MD5-96 authentication level. **<auth_password 8-16>** - Enter the MD5 authentication password here. This value must be between 8 and 16 characters. **sha** - The HMAC-SHA-96 authentication level. **<auth_password 8-20>** - Enter the SHA authentication password here. This value must be between 8 and 20 characters.
priv - (Optional) A privacy key used by DES, it is hex string type. **none** - Specify that no encryption will be used for the privacy key. **des** - Specify that the DES encryption will be used for the privacy key. **<priv_password 8-16>** - Enter the DES password value here. This value must be between 8 and 16 characters long.
by_key - (Optional) Indicate input key for authentication and privacy. **auth** - An authentication string used by MD5 or SHA1. **md5** - An authentication key used by MD5, it is hex string type. **<auth_key 32-32>** - Enter the MD5 authentication key here. This value must be 32 characters long. **sha** - An authentication key used by SHA1, it is hex string type. **<auth_key 40-40>** - Enter the SHA authentication key here. This value must be 32 characters long.
priv - (Optional) A privacy key used by DES, it is hex string type. **none** - Specify that no encryption will be used for the privacy key.

des - Specify that the DES encryption will be used for the privacy key.
<priv_key 32-32> - Enter the DES privacy key here. This value must be 32 characters long.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a SNMP user “user123” with group “group123”:

```
DES-3200-28P:admin#create snmp user user123 group123 encrypted by_password auth
md5 12345678 priv des 12345678
Command: create snmp user user123 group123 encrypted by_password auth md5
12345678 priv des 12345678

Success.

DES-3200-28P:admin#
```

63-5 delete snmp user

Description

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

Format

delete snmp user <username 32>

Parameters

<username 32> - The name of the user on the host that connects to the agent. The range is 1 to 32.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a SNMP user “user123”:

```
DES-3200-28P:admin#delete snmp user user123
Command: delete snmp user user123

Success.

DES-3200-28P:admin#
```

63-6 show snmp user

Description

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

Format

show snmp user

Parameters

None.

Restrictions

None.

Example

To show SNMP user:

```
DES-3200-28P:admin#show snmp user
Command: show snmp user

Username                          Group Name             VerAuthPriv
--------------------------------  -------------------------  -----------
initial                           initial                V3 NoneNone
user123                           group123               V3 MD5 DES

Total Entries : 2

DES-3200-28P:admin#
```

63-7 create snmp group

Description

This command is used to create a new SNMP group, or a table that maps SNMP users to SNMP views.

Format

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

Parameters

group - Specify the name of the group. **<groupname 32>** - Enter the group name here. This name can be up to 32 characters long.
v1 - The least secure of the possible security models.

v2c - The second least secure of the possible security models.
v3 - The most secure of the possible.
noauth_nopriv - Neither support packet authentication nor encrypting. **auth_nopriv** - Support packet authentication. **auth_priv** - Support packet authentication and encrypting.
read_view - (Optional) Specify that the view name would be read. **<view_name 32>** - Enter the read view name here. This name can be up to 32 characters long.
write_view - (Optional) Specify that the view name would be write. **<view_name 32>** - Enter the wite view name here. This name can be up to 32 characters long.
notify_view - (Optional) Specify that the view name would be notify. **<view_name 32>** - Enter the notify view name here. This name can be up to 32 characters long.

Restrictions

Only Administrator-level users can issue this command.

Example

To create SNMP group “group123”:

```
DES-3200-28P:admin#create snmp group group123 v3 auth_priv read_view
CommunityView write_view CommunityView notify_view CommunityView

Command: create snmp group group123 v3 auth_priv read_view CommunityView
write_view CommunityView notify_view CommunityView


Success.


DES-3200-28P:admin#
```

63-8 delete snmp group

Description

This command is used to remove a SNMP group.

Format

delete snmp group <groupname 32>

Parameters

<groupname 32> - The name of the group will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete SNMP group “group123”:

```
DES-3200-28P:admin#delete snmp group group123
Command: delete snmp group group123

Success.

DES-3200-28P:admin#
```

63-9 show snmp groups

Description

This command is used to display the names of groups on the Switch and the security model, level, the status of the different views.

Format

show snmp groups

Parameters

None.

Restrictions

None.

Example

To show SNMP groups:

```
DES-3200-28P:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

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

Group    Name      : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name : CommunityView
Securiy Model     : SNMPv2
Securiy Level     : NoAuthNoPriv

Group    Name      : initial
ReadView Name     : restricted
WriteView Name    :
Notify View Name : restricted
Securiy Model     : SNMPv3
Securiy Level     : NoAuthNoPriv

Group    Name      : WriteGroup
ReadView Name     : CommunityView
WriteView Name    : CommunityView
Notify View Name : CommunityView
Securiy Model     : SNMPv2
Securiy Level     : NoAuthNoPriv

Total Entries: 10

DES-3200-28P:admin#
```

63-10 create snmp view

Description

This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.

Format

create snmp view <view_name 32> <oid> view_type [included | excluded]

Parameters

view - View name to be created. **<view_name 32>** - Enter the view name here. The name can be up to 32 characters long.

<oid> - Object-Identified tree, MIB tree.
view_type - Specify the access type of the MIB tree in this view. **included** - Includes for this view. **excluded** - Excluded for this view.

Restrictions

Only Administrator-level users can issue this command.

Example

To create SNMP view “view123”:

```
DES-3200-28P:admin#create snmp view view123 1.3.6 view_type included
Command: create snmp view view123 1.3.6 view_type included

Success.

DES-3200-28P:admin#
```

63-11 delete snmp view

Description

This command is used to remove a view record.

Format

delete snmp view <view_name 32> [all | <oid>]

Parameters

view - View name to be deleted. **<view_name 32>** - Enter the view name here. The name can be up to 32 characters long.
all - Specify that all view records will be removed. **<oid>** - Object-Identified tree, MIB tree.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete SNMP view “view123”:

```
DES-3200-28P:admin#delete snmp view view123 all
Command: delete snmp view view123 all

Success.

DES-3200-28P:admin#
```

63-12 show snmp view

Description

This command is used to display the SNMP view record.

Format

show snmp view {<view_name 32>}

Parameters

view - (Optional) View name of the user who likes to show. **<view_name 32>** - Enter the view name here. The name can be up to 32 characters long.

Restrictions

None.

Example

To show SNMP view:

```
DES-3200-28P:admin#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name              Subtree                   View Type
---------------------  ------------------------  ----------
view123                1.3.6                     Included
restricted             1.3.6.1.2.1.1             Included
restricted             1.3.6.1.2.1.11            Included
restricted             1.3.6.1.6.3.10.2.1        Included
restricted             1.3.6.1.6.3.11.2.1        Included
restricted             1.3.6.1.6.3.15.1.1        Included
CommunityView          1                         Included
CommunityView          1.3.6.1.6.3               Excluded
CommunityView          1.3.6.1.6.3.1             Included

Total Entries: 9

DES-3200-28P:admin#
```

63-13 create snmp host

Description

This command is used to create a recipient of an SNMP trap operation.

Format

create snmp host <ipaddr> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string32>

Parameters

<ipaddr> - The IP address of the recipient for which the traps are targeted.
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 32> - Authentication string. If the v1 or v2 is specified, the auth_string presents the community string, and it must be one of the entries in community table. If the v3 is specified, the auth_string presents the user name, and it must be one of the entries in the user table.

Restrictions

Only Administrator-level users can issue this command.

Example

To create SNMP host “10.0.0.1” with community string “public”:

```
DES-3200-28P:admin#create snmp host 10.0.0.1 v1 public
Command: create snmp host 10.0.0.1 v1 public

Success.

DES-3200-28P:admin#
```

63-14 delete snmp host

Description

This command is used to delete a recipient of an SNMP trap operation.

Format

delete snmp host <ipaddr>

Parameters

<ipaddr> - Enter the IP address of the recipient for which the traps are targeted.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete SNMP host “10.0.0.1”:

```
DES-3200-28P:admin#delete snmp host 10.0.0.1
Command: delete snmp host 10.0.0.1

Success.

DES-3200-28P:admin#
```

63-15 show snmp host

Description

This command is used to display the recipient for which the traps are targeted.

Format

show snmp host {<ipaddr>}

Parameters

host - (Optional) The IP address of the recipient for which the traps are targeted. **<ipaddr>** - Enter the IP address used for the configuration here.
If no parameter specified, all SNMP hosts will be displayed.

Restrictions

None.

Example

To show SNMP host:

```
DES-3200-28P:admin#show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  ---------------------------------
10.90.90.3        V3 noauthnopriv  initial
10.90.90.2        V2c                private
10.90.90.1        V1                 public
10.90.90.4        V3 authnopriv    user123
10.90.90.5        V3 authpriv      user234

Total Entries : 5

DES-3200-28P:admin#
```

63-16 config snmp engineID

Description

This command is used to configure a identifier for the SNMP engine on the Switch.

Format

config snmp engineID <snmp_engineID 10-64>

Parameters

engineID - Identify for the SNMP engine on the Switch. It is octet string type. It accepts the hex number directly.
<snmp_engineID 10-64> - Enter the SNMP engine ID here. This value must be between 10 and 64.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure SNMP engine ID to “1023457890”:

```
DES-3200-28P:admin#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DES-3200-28P:admin#
```

63-17 show snmp engineID

Description

The show snmp engineID command displays the identification of the SNMP engine on the Switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent’s SNMP management private enterprise number as assigned by IANA, D_Link is 171. The fifth octet is 03 to indicates the rest is the MAC address of this device. The 6th –11th octets is MAC address.

Format

show snmp engineID

Parameters

None.

Restrictions

None.

Example

To show SNMP engine ID:

```
DES-3200-28P:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DES-3200-28P:admin#
```

63-18 enable snmp

Description

This command is used to enable the SNMP function.

Format

enable snmp

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable SNMP:

```
DES-3200-28P:admin#enable snmp
Command: enable snmp

Success.

DES-3200-28P:admin#
```

63-19 disable snmp

Description

This command is used to disable the SNMP function.

Format

disable snmp

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To disable SNMP:

```
DES-3200-28P:admin#disable snmp
Command: disable snmp

Success.

DES-3200-28P:admin#
```

63-20 config snmp system_name

Description

This command is used to configure the name for the Switch.

Format

config snmp system_name {<sw_name>}

Parameters

system_name - A maximum of 128 characters is allowed. And NULL string is accepted. **<sw_name>** - (Optional) Enter the system name used here.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure the Switch name for “DES-32xx L2 Switch”:

```
DES-3200-28P:admin#config snmp system_name DES-32xx L2 Switch
Command: config snmp system_name DES-32xx L2 Switch

Success.

DES-3200-28P:admin#
```

63-21 config snmp system_location

Description

This command is used to enter a description of the location of the Switch.

Format

config snmp system_location {<sw_location>}

Parameters

system_location - A maximum of 128 characters is allowed. And NULL string is accepted
<sw_location> - (Optional) Enter the system location string here.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure the Switch location for “HQ 5F”:

```
DES-3200-28P:admin#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3200-28P:admin#
```

63-22 config snmp system_contact

Description

This command is used to enter the name of a contact person who is responsible for the Switch.

Format

config snmp system_contact {<sw_contact>}

Parameters

system_contact - A maximum of 128 characters is allowed. And NULL string is accepted.
<sw_contact> - (Optional) Enter the system contact string here.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure the Switch contact to “MIS Department II”:

```
DES-3200-28P:admin#config snmp system_contact "MIS Department II"
Command: config snmp system_contact "MIS Department II"

Success.

DES-3200-28P:admin#
```

63-23 enable snmp traps

Description

This command is used to enable SNMP trap support.

Format

enable snmp traps

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable SNMP trap support:

```
DES-3200-28P:admin#enable snmp traps
Command: enable snmp traps

Success.

DES-3200-28P:admin#
```

63-24 disable snmp traps

Description

This command is used to disable SNMP trap support on the Switch.

Format

disable snmp traps

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To prevent SNMP traps from being sent from the Switch:

```
DES-3200-28P:admin#disable snmp traps
Command: disable snmp traps

Success.

DES-3200-28P:admin#
```

63-25 enable snmp authenticate_traps

Description

This command is used to enable SNMP authentication failure trap support.

Format

enable snmp authenticate_traps

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable SNMP authentication trap support:

```
DES-3200-28P:admin#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DES-3200-28P:admin#
```

63-26 disable snmp authenticate_traps

Description

This command is used to disable SNMP authentication failure trap support.

Format

disable snmp authenticate_traps

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To disable SNMP authentication trap support:

```
DES-3200-28P:admin#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DES-3200-28P:admin#
```

63-27 enable snmp linkchange_traps

Description

This command is used to configure the sending of linkchange traps.

Format

enable snmp linkchange_traps

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable the sending of linkchange traps:

```
DES-3200-28P:admin#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DES-3200-28P:admin#
```

63-28 disable snmp linkchange_traps

Description

This command is used to configure the sending of linkchange traps.

Format

disable snmp linkchange_traps

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To disable the sending of linkchange traps:

```
DES-3200-28P:admin#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DES-3200-28P:admin#
```

63-29 config snmp linkchange_traps ports

Description

This command is used to configure the sending of linkchange traps and per port control for sending of change trap.

Format

config snmp linkchange_traps ports [all | <portlist>] [enable | disable]

Parameters

all - To specify all ports. **<portlist>** - To specify a port range.
enable - Enable sending of the link change trap for this port. **disable** - Disable sending of the link change trap for this port.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the sending of linkchange traps:

```
DES-3200-28P:admin#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DES-3200-28P:admin#
```

63-30 config snmp coldstart_traps

Description

This command is used to configure the trap for coldstart event.

Format

config snmp coldstart_traps [enable | disable]

Parameters

enable - Enable the trap of the coldstart event. The default state is enabled. **disable** - Disable the trap of the coldstart event.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the trap for coldstart event:

```
DES-3200-28P:admin#config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

DES-3200-28P:admin#
```

63-31 config snmp warmstart_traps

Description

This command is used to configure the trap state for warmstart event.

Format

config snmp warmstart_traps [enable | disable]

Parameters

enable - Enable the trap of the warmstart event. The default state is enabled. **disable** - Disable the trap of the warmstart event.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the trap state for warmstart event:

```
DES-3200-28P:admin#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DES-3200-28P:admin#
```

63-32 show snmp traps

Description

This command is used to display the snmp trap sending status.

Format

show snmp traps {linkchange_traps {ports <portlist>}}

Parameters

linkchange_traps - (Optional) Specify that the SNMP trap sending status will be displayed.
ports - (Optional) Specify the ports for the display. **<portlist>** - Enter the list of ports used for the display here.

Restrictions

None.

Example

```
DES-3200-28P:admin#show snmp traps
Command: show snmp traps

SNMP Traps         : Enabled
Authenticate Trap  : Enabled
Linkchange Traps   : Enabled
Coldstart Traps    : Enabled
Warmstart Traps    : Enabled

DES-3200-28P:admin#
```

63-33 config rmon trap

Description

This command is used to configure the trap state for RMON events.

Format

config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]} (1)

Parameters

rising_alarm - (Optional) Specify the trap state for rising alarm. The default state is enabled. **enable** - Specify that the rising alarm function will be enabled. **disable** - Specify that the rising alarm function will be disabled.
falling_alarm - (Optional) Specify the trap state for falling alarm. The default state is enabled. **enable** - Specify that the falling alarm function will be enabled. **disable** - Specify that the falling alarm function will be disabled.

Restrictions

Only Administrator level can issue this command.

Example

To configure the trap state for RMON events:

```
DES-3200-28P:admin#config rmon trap rising_alarm disable
Command: config rmon trap rising_alarm disable

Success.

DES-3200-28P:admin#
```

63-34 show rmon

Description

This command is used to display the RMON related setting.

Format

show rmon

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the RMON related setting:

```
DES-3200-28P:admin#show rmon
Command: show rmon

RMON Rising Alarm Trap      : Enabled
RMON Falling Alarm Trap     : Enabled

DES-3200-28P:admin#
```

Chapter 64 Single IP Management Command List

enable sim
disable sim
show sim {[candidates {<candidate_id 1-100>} | members{<member_id 1-32>} | group {commander_mac <macaddr>} | neighbor]}
reconfig {member_id <value 1-32> | exit}
config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]
config sim [{[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>}]
download sim_ms [firmware_from_tftp | configuration_from_tftp] {<ipaddr> <path_filename> {[members <mslist 1-32> | all]}}
upload sim_ms [configuration_to_tftp | log_to_tftp] {<ipaddr> <path_filename> {[members <mslist> | all]}}
config sim trap [enable | disable]

64-1 enable sim

Description

This command is used to configure the single IP management on the Switch as enabled.

Format

enable sim

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SIM:

```
DES-3200-28P:admin#enable sim
Command: enable sim

Success.

DES-3200-28P:admin#
```

64-2 disable sim

Description

This command is used to disable single IP management on the Switch.

Format

disable sim

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SIM:

```
DES-3200-28P:admin#disable sim
Command: disable sim

Success.

DES-3200-28P:admin#
```

64-3 show sim

Description

This command is used to display the current information of the specific sort of devices.

Format

show sim {[candidates {<candidate_id 1-100>} | members{<member_id 1-32>} | group {commander_mac <macaddr>} | neighbor]}

Parameters

candidates - (Optional) Specify the candidate devices. **<candidate_id 1-100>** - (Optional) Enter the candidate device ID here. This value must be between 1 and 100.
members - (Optional) Specify the member devices. **<member_id 1-32>** - (Optional) Enter the member device ID here. This value must be between 1 and 32.
group - (Optional) Specify other group devices. **commander_mac** - (Optional) Specify the commander MAC address used. **<macaddr>** - Enter the commander MAC address used here.
neighbor - (Optional) Specify other neighbor devices.

Restrictions

None.

Example

To show the self information in detail:

```
DES-3200-28P:admin#show sim
Command: show sim

SIM Version        : VER-1.61
Firmware Version   : 4.03.004
Device Name        : DES-3200-28P
MAC Address        : 00-01-02-03-04-00
Capabilities       : L2
Platform           : DES-3200-28P L2 Switch
SIM State          : Enabled
Role State         : Candidate
Discovery Interval : 30 sec
Hold Time          : 100 sec

DES-3200-28P:admin#
```

To show the candidate information in summary, if user specify candidate id, it would show information in detail:

```
DES-3200-28P:admin#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 DES-XXXXS L2 Switch      40    1.00-B01 aaaaaaaaaaaaaaaa
                                                              bbbbbbbbbbbbbbb
 2  00-55-55-00-55-00 DES-3326SR L3 Switch     140   4.00-B15 default master

Total Entries: 2

DES-3200-28P:admin#
```

To show the member information in summary, if user specify member id, it will show information in detail:

```
DES-3200-28P:admin#show sim member
Command: show sim member

ID  MAC Address       Platform /               Hold  Firmware Device Name
Capability               Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
 1  00-01-02-03-04-00 DES-XXXXS L2 Switch      40    1.00-B01 aaaaaaaaaaaaaaaa
                                                               bbbbbbbbbbbbbbb
 2  00-55-55-00-55-00 DES-3326SR L3 Switch     140   4.00-B15 default master

Total Entries: 2

DES-3200-28P:admin#
```

To show other groups information in summary, if user specify group name, it will show information in detail:

```
DES-3200-28P:admin#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address       Platform /               Hold  Firmware Device Name
Capability               Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
*1  00-01-02-03-04-00 DES-XXXXS L2 Switch      40    1.00-B01 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 DES-XXXXS L2 Switch      40    1.00-B01 aaaaaaaaaaaaaaaa
                                                               bbbbbbbbbbbbbbb
  2  00-55-55-00-55-00
  3  00-55-55-00-55-11

Total Entries: 2

DES-3200-28P:admin#
```

To show neighbor table of SIM:

```
DES-3200-28P:admin#show sim neighbor
Command: show sim neighbor

Neighbor Table

Port    MAC Address         Role
------  ------------------  ---------
23      00-35-26-00-11-99   Commander
23      00-35-26-00-11-91   Member
24      00-35-26-00-11-90   Candidate

Total Entries: 3

DES-3200-28P:admin#
```

64-4 reconfig

Description

This command is used to re-telnet to member.

Format

reconfig {member_id <value 1-32> | exit}

Parameters

member_id - (Optional) Specify the serial number of the member. **<value 1-32>** - Enter the serial number of the member here.
exit - (Optional) Specify to exit from the telnet session.

Restrictions

Only Administrator-level users can issue this command.

Example

To re-telnet to member:

```
DES-3200-28P:admin#reconfig member_id 1
Command: reconfig member_id 1

DES-3200-28P:admin#
Login:
```

64-5 config sim_group

Description

This command is used to configure group information.

Format

config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]

Parameters

add - Specify to add a specific candidate to the group. **<candidate_id 1-100>** - Enter the candidate ID to be added to the group here. This value must be between 1 and 100.
<password> - (Optional) The password of candidate if necessary.
delete - Specify to delete a member from the group. **<member_id 1-32>** - Enter the member ID of the member to be removed from the group here. This value must be between 1 and 32.

Restrictions

Only Administrator-level users can issue this command.

Example

To add a member:

```
DES-3200-28P:admin#config sim_group add 2
Command: config sim_group add 2

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DES-3200-28P:admin#
```

To delete a member:

```
DES-3200-28P:admin#config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DES-3200-28P:admin#
```

64-6 config sim

Description

This command is used to configure the role state and the parameters of the discovery protocol on the Switch.

Format

config sim [{[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>}]

Parameters

commander - (Optional) Specify to transfer the role to the commander.
group_name - (Optional) Specify that if the user is the commander, the user can update the name of group. **<groupname 64>** - Enter the group name here. This name can be up to 64 characters long.
candidate - (Optional) Specify to transfer the role to the candidate.
dp_interval - (Optional) The time in seconds between discoveries. **<sec 30-90>** - Enter the discovery time here in seconds. This value must be between 30 and 90 seconds.
hold_time - (Optional) The time in seconds the device holds the discovery result. **<sec 100-255>** - Enter the hold time here in seconds. This value must be between 100 and 255.

Restrictions

Only Administrator level can issue this command.

Example

To transfer to commander:

```
DES-3200-28P:admin#config sim commander
Command: config sim commander

Success.

DES-3200-28P:admin#
```

To transfer to candidate:

```
DES-3200-28P:admin#config sim candidate
Command: config sim candidate

Success.

DES-3200-28P:admin#
```

To update name of group:

```
DES-3200-28P:admin#config sim commander group_name mygroup
Command: config sim commander group_name mygroup

Success.

DES-3200-28P:admin#
```

To change the time interval of discovery protocol:

```
DES-3200-28P:admin#config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DES-3200-28P:admin#
```

To change the hold time of discovery protocol:

```
DES-3200-28P:admin#config sim hold_time 200
Command: config sim hold_time 200

Success.

DES-3200-28P:admin#
```

64-7 download sim_ms

Description

This command is used to download firmware or configuration to indicated device.

Format

download sim_ms [firmware_from_tftp | configuration_from_tftp] {<ipaddr> <path_filename> {[members <mslist 1-32> | all]}}

Parameters

firmware_from_tftp - Specify that the firmware will be downloaded from the TFTP server.
configuration_from_tftp - Specify that the configuration will be downloaded from the TFTP server.
<ipaddr> - (Optional) Specify the IP address of the TFTP server. **<path_filename>** - (Optional) Specify the file path of the firmware or configuration in the TFTP server. **members** - (Optional) Specify a range of members who can download this firmware or configuration. **<mslist 1-32>** - Enter the member list used here. This value must be between 1 and 32. **all** - (Optional) Specify that all members will be used.

Restrictions

Only Administrator-level users can issue this command.

Example

To download configuration:

```
DES-3200-28P:admin#download sim_ms configuration_from_tftp 10.55.47.1
D:\dwl600x.tfp members 1
Commands: download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp
members 1

This device is updating configuration.  Please wait several minutes ...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success

DES-3200-28P:admin#
```

To download firmware:

```
DES-3200-28P:admin#download sim_ms firmware_from_tftp 10.55.47.1 D:\test.txt
members 1
Commands: download sim_ms firmware_from_tftp 10.55.47.1 D:\test.txt members 1

This device is updating firmware.  Please wait several minutes ...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success

DES-3200-28P:admin#
```

64-8 upload sim_ms

Description

This command is used to upload configuration to TFTP server.

Format

upload sim_ms [configuration_to_tftp | log_to_tftp] {<ipaddr> <path_filename> {[members <mslist> | all]}}

Parameters

configuration_to_tftp - Specify that the configuration will be uploaded to the TFTP server.
log_to_tftp – Specify that the log file will be uploaded to the TFTP server.
<ipaddr> - (Optional) Specify the IP address of the TFTP server. **<path_filename>** - Specify the file path to store the configuration in the TFTP server. **members** - (Optional) Specify a range of members who can up this configuration. **<mslist>** - (Optional) Enter the member list used here. **all** - (Optional) Specify that all members will be used.

Restrictions

Only Administrator-level users can issue this command.

Example

To upload configuration:

```
DES-3200-28P:admin#upload sim_ms configuration_to_tftp 10.55.47.1
D:\configuration.txt members 1
Command: upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt
members 1

This device is uploading configuration.  Please wait several minutes ...

Upload Status :

ID   MAC Address       Result
---  ----------------- ----------------
1   00-1A-2D-00-12-12 Success

DES-3200-28P:admin#
```

64-9 config sim trap

Description

This command is used to control sending of traps issued from the member switch.

Format

config sim trap [enable | disable]

Parameters

enable - Enable the trap state.
disable - Disable the trap state.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To enable sim trap:

```
DES-3200-28P:admin#config sim trap enable
Command: config sim trap enable

Success.

DES-3200-28P:admin#
```

Chapter 65 Syslog and Trap Source-interface Command List

config syslog source_ipif [<ipif_name 12> {<ipaddr>} | none]
show syslog source_ipif
config trap source_ipif [<ipif_name 12> {<ipaddr>} | none]
show trap source_ipif

65-1 config syslog source_ipif

Description

This command is used to configure syslog source IP interface.

Format

config syslog source_ipif [<ipif_name 12> {<ipaddr>} | none]

Parameters

ipif - Specify the IP interface name. If only specify this parameter, the least IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long. **<ipaddr>** - (Optional) Enter the IP address used for the configuration here. **none** - Specify to clear the configured source IP interface.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

Configure syslog source IP interface:

```
DES-3200-28P:admin#config syslog source_ipif ipif3 14.0.0.5
Command: config syslog source_ipif ipif3 14.0.0.5

Success

DES-3200-28P:admin#
```

To clear the configured source IP interface for syslog:

```
DES-3200-28P:admin#config syslog source_ipif none
Command: config syslog source_ipif none

Success

DES-3200-28P:admin#
```

65-2 show syslog source_ipif

Description

This command is used to display the syslog source IP interface.

Format

show syslog source_ipif

Parameters

None.

Restrictions

None.

Example

Show syslog source IP interface:

```
DES-3200-28P:admin#show syslog source_ipif
Command: show syslog source_ipif

 Syslog Source IP Interface Configuration:

 IP Interface           : ipif3
 IPv4 Address           : 14.0.0.5

DES-3200-28P:admin#
```

65-3 config trap source_ipif

Description

This command is used to configure trap source IP interface.

Format

config trap source_ipif [<ipif_name 12> {<ipaddr>} | none]

Parameters

ipif - Specify the IP interface name. If only specify this parameter, the least IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long. **<ipaddr>** - (Optional) Enter the IP address used for the configuration here. **none** - Specify to clear the configured source IP interface.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

Configure trap source IP interface:

```
DES-3200-28P:admin#config trap source_ipif System
Command: config trap source_ipif System

Success

DES-3200-28P:admin#
```

To clear the configured trap source IP interface:

```
DES-3200-28P:admin#config trap source_ipif none
Command: config trap source_ipif none

Success

DES-3200-28P:admin#
```

65-4 show trap source_ipif

Description

This command is used to display the trap source IP interface.

Format

show trap source_ipif

Parameters

None.

Restrictions

None.

Example

Show trap source IP interface:

```
DES-3200-28P:admin#show trap source_ipif
Command: show trap source_ipif

Trap Source IP Interface Configuration:

IP Interface           : System
IPv4 Address           : None

DES-3200-28P:admin#
```

Chapter 66 System Log Command List

clear log
show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module<module_list>]}
show log_software_module
enable syslog
disable syslog
show syslog
create syslog host <index 1-4> ipaddress <ipaddr> {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}
config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | 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
show attack_log {index <value_list>}
clear attack_log

66-1 clear log

Description

This command is used to clear the Switch's history log.

Format

clear log

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To clear the Switch's history log:

```
DES-3200-28P:admin#clear log
Command: clear log

Success.

DES-3200-28P:admin#
```

66-2 show log

Description

This command is used to display the Switch's history log.

Format

show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module<module_list>]}

Parameters

index - (Optional) The show log command will display the history log between the log number of X and Y. For example, showing log index 1-5 will display the history log from 1 to 5. **<value_list>** - Enter the index value here.
severity - (Optional) Specify the severity level used.
module - (Optional) Specify the modules which are to be displayed. The module can be obtained by using the show log_software_module command. Use a comma to separate multiple modules. **<module_list>** - Enter the module list value here.
emergency - (Optional) Severity level 0 **alert** - (Optional) Severity level 1 **critical** - (Optional) Severity level 2 **error** - (Optional) Severity level 3 **warning** - (Optional) Severity level 4 **notice** - (Optional) Severity level 5 **informational** - (Optional) Severity level 6 **debug** - (Optional) Severity level 7 **<level_list 0-7>** - Specify a list of severity level which is to be displayed. If there is more than one severity level, please separate them by comma. The level number is from 0 to 7.
module - (Optional) Specify the modules which are to be displayed. The module can be obtained by using the show log_software_module command. Use a comma to separate multiple modules. **<module_list>** - Enter the module list value here.
If no parameter is specified, all history log entries will be displayed.

Restrictions

None.

Example

To display the Switch's history log:

```
DES-3200-28P:admin#show log index 1-3
Command: show log index 1-3

Index Date       Time     Level   Log Text
----- ---------- -------- ------- --------------------------------------------

3     2000-01-01 00:00:40 CRIT(2) System started up
2     2000-01-01 00:00:40 CRIT(2) System cold start
1     2000-01-01 01:49:30 INFO(6) Anonymous: execute command "reset system".

DES-3200-28P:admin#
```

66-3 show log_software_module

Description

This command is used to display the protocols or applications that support the enhanced log. The enhanced log adds the module name and module ID. Network administrators can display logs by module name or module ID.

Format

show log_software_module

Parameters

None.

Restrictions

None.

Example

To display the protocols or applications that support the enhanced log:

```
DES-3200-28P:admin#show log_software_module
Command: show log_software_module

ERPS                ERROR_LOG           MSTP

DES-3200-28P:admin#
```

66-4 enable syslog

Description

This command is used to enable the sending of syslog messages.

Format

enable syslog

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable the sending of syslog messages:

```
DES-3200-28P:admin#enable syslog
Command: enable syslog

Success.

DES-3200-28P:admin#
```

66-5 disable syslog

Description

This command is used to disable the sending of syslog messages.

Format

disable syslog

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To disable the sending of syslog messages:

```
DES-3200-28P:admin#disable syslog
Command: disable syslog

Success.

DES-3200-28P:admin#
```

66-6 show syslog

Description

This command is used to display the syslog protocol global state.

Format

show syslog

Parameters

None.

Restrictions

None.

Example

To display the syslog protocol global state:

```
DES-3200-28P:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-3200-28P:admin#
```

66-7 create syslog host

Description

This command is used to create a new syslog host. The user can choose and report specific levels of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to that host.

Format

create syslog host <index 1-4> ipaddress <ipaddr> {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}

Parameters

<index 1-4> - Enter the host index value here.
ipaddress - Specify the IP address for the host. **<ipaddr>** - Specify the IP address for the host.
severity - (Optional) Specify the severity level. **emergency** - Severity level 0 **alert** - Severity level 1 **critical** - Severity level 2

error - Severity level 3 **warning** - Severity level 4 **notice** - Severity level 5 **informational** - Severity level 6 **debug** - Severity level 7 **<level 0-7>** - Enter the severity level value here. This value must be between 0 and 7.
facility - (Optional) Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown below. This facility setting will be put in the syslog packet when it is sent to a specific syslog server. **local0** - Specify that the user-defined facility will be set to local 0. **local1** - Specify that the user-defined facility will be set to local 1. **local2** - Specify that the user-defined facility will be set to local 2. **local3** - Specify that the user-defined facility will be set to local 3. **local4** - Specify that the user-defined facility will be set to local 4. **local5** - Specify that the user-defined facility will be set to local 5. **local6** - Specify that the user-defined facility will be set to local 6. **local7** - Specify that the user-defined facility will be set to local 7.
udp_port - (Optional) Specify the UDP port number. **<udp_port_number>** - Enter the UDP port number used here.
state - (Optional) The syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages. **enable** - Specify that the host to receive such messages will be enabled. **disable** - Specify that the host to receive such messages will be disabled.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

Adds a new syslog host:

```
DES-3200-28P:admin#create syslog host 1 ipaddress 10.90.90.1 severity debug
facility local0
Command: create syslog host 1 ipaddress 10.90.90.1 severity debug facility
local0

Success.

DES-3200-28P:admin#
```

66-8 config syslog host

Description

This command is used to configure the syslog host configurations. The user can choose and report a specific level of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to the specified host.

Format

config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 |

local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}

Parameters

<index> - Enter the host index value here.
all - Specify that all the host indexes will be used.
severity - (Optional) Specify the severity level. **emergency** - Severity level 0 **alert** - Severity level 1 **critical** - Severity level 2 **error** - Severity level 3 **warning** - Severity level 4 **notice** - Severity level 5 **informational** - Severity level 6 **debug** - Severity level 7 **<level 0-7>** - Enter the severity level value here. This value must be between 0 and 7.
facility - (Optional) Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown below. This facility setting will be put in the syslog packet when it is sent to a specific syslog server. **local0** - Specify that the user-defined facility will be set to local 0. **local1** - Specify that the user-defined facility will be set to local 1. **local2** - Specify that the user-defined facility will be set to local 2. **local3** - Specify that the user-defined facility will be set to local 3. **local4** - Specify that the user-defined facility will be set to local 4. **local5** - Specify that the user-defined facility will be set to local 5. **local6** - Specify that the user-defined facility will be set to local 6. **local7** - Specify that the user-defined facility will be set to local 7.
udp_port - (Optional) Specify the UDP port number. **<udp_port_number>** - Enter the UDP port number used here.
ipaddress - (Optional) Specify IP address for the host. **<ipaddr>** - Enter the IP address used for the configuration here.
state - (Optional) The syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages. **enable** - Specify that the host to receive such messages will be enabled. **disable** - Specify that the host to receive such messages will be disabled.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure the syslog host configuration:

```
DES-3200-28P:admin#config syslog host all severity debug facility local0
Command: config syslog host all severity debug facility local0

Success.

DES-3200-28P:admin#
```

66-9 delete syslog host

Description

This command is used to delete the syslog host(s).

Format

delete syslog host [<index 1-4> | all]

Parameters

host - The host index or all hosts. **<index>** - Enter the host index value here. **all** - Specify that all the host indexes will be used.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To delete the specific syslog host:

```
DES-3200-28P:admin#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3200-28P:admin#
```

66-10 show syslog host

Description

This command is used to display the syslog host configurations.

Format

show syslog host {<index 1-4>}

Parameters

host - The host index or all hosts. **<index>** - (Optional) Enter the host index value here.
If no parameter is specified, all hosts will be displayed.

Restrictions

None.

Example

To show the syslog host information:

```
DES-3200-28P:admin#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host  1
  IP Address        : 10.90.90.1
  Severity          : Debug(7)
  Facility          : Local0
  UDP Port          : 514
  Status            : Disabled

Total Entries : 1

DES-3200-28P:admin#
```

66-11 config log_save_timing

Description

This command is used to set the method for saving the log.

Format

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

Parameters

time_interval - Save log to flash every xxx minutes. (If no new log events occur in this period, don't save.) **<min 1-65535>** - Enter the time interval value here. This value must be between 1 and 65535 minutes.
on_demand - Save log to flash whenever the user enters the "save log" or "save all" command. The default setting is on_demand.
log_trigger - Save log to flash whenever a new log event arrives.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure the method for saving a log as on demand:

```
DES-3200-28P:admin#config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DES-3200-28P:admin#
```

66-12 show log_save_timing

Description

This command is used to show the method for saving the log.

Format

show log_save_timing

Parameters

None.

Restrictions

None.

Example

To show the timing method used for saving the log:

```
DES-3200-28P:admin#show log_save_timing
Command: show log_save_timing

Saving Log Method: On_demand

DES-3200-28P:admin#
```

66-13 show attack_log

Description

This command is used to display the attack log messages. The attack log message refers to log messages driven by modules such as DOS and the IP-MAC-port binding module. This type of log message may generate a large amount of messages and quickly cause the system to run out of system log storage. Therefore, for this type of log messages only the first log that is generated each minute can be stored in the system log, with the rest of them being stored in a separate table named attack log.

Format

show attack_log {index <value_list>}

Parameters

index - (Optional) The list of index numbers of the entries that need to be displayed. For example, show attack_log index 1-5 will display the attack log messages from 1 to 5. **<value_list>** - Enter the index numbers of the entries that needs to be displayed here.
If no parameter is specified, all entries in the attack log will be displayed.

Restrictions

None.

Example

To show dangerous messages on the master:

```
DES-3200-28P:admin#show attack_log index 1
Command: show attack_log index 1

Index   Date       Time      Level     Log Text
----- ---------- -------- -------- ------------------------------------------
1      2008-10-17 15:00:14 CRIT(2)   Possible spoofing attack from IP: , MAC:
                                     0A-00-00-5A-00-01, port: 3

DES-3200-28P:admin#
```

66-14 clear attack_log

Description

This command is used to clear the attack log.

Format

clear attack_log

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To clear the master's attack log:

```
DES-3200-28P:admin#clear attack_log
Command: clear attack_log

Success.

DES-3200-28P:admin#
```

Chapter 67 System Severity Command List

config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]
show system_severity

67-1 config system_severity

Description

This command is used to configure the severity level control for the system.

When the user chooses a specific level to log or trap, messages at that severity level or more will be logged or trapped to SNMP managers.

Format

config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]

Parameters

trap - Specify the severity level control for traps.
log - Specify the severity level control for the log.
all - Specify the severity level control for traps and the log.
emergency - Severity level 0. **alert** - Severity level 1. **critical** - Severity level 2. **error** - Severity level 3. **warning** - Severity level 4. **notice** - Severity level 5. **information** - Severity level 6. **debug** - Severity level 7. **<level 0-7>** - Enter the severity level here. This value must be between 0 and 7.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure severity level control as information level for trap:

```
DES-3200-28P:admin#config system_severity trap warning
Command: config system_severity trap warning

Success.

DES-3200-28P:admin#
```

67-2 show system_severity

Description

This command is used to display the severity level controls for the system.

Format

show system_severity

Parameters

None.

Restrictions

None.

Example

To show severity level control for system:

```
DES-3200-28P:admin#show system_severity
Command: show system_severity

System Severity Trap : warning(4)
System Severity Log : information(6)

DES-3200-28P:admin#
```

Chapter 68 Telnet Client Command List

telnet <ipaddr> {tcp_port <value 1-65535>}

68-1 telnet

Description

This command is used to start the telnet client to connect to the specific telnet server. The parameters specified by the command will only be used for the establishment of this specific session. They will not affect the establishment of other sessions.

Format

telnet <ipaddr> {tcp_port <value 1-65535>}

Parameters

<ipaddr> - The IP address of the telnet server.
tcp_port - (Optional) Specify the telnet server port number to be connected. If not specified, the default port is 23. **<value 1-65535>** - Enter the TCP port number used here. This value must be between 1 and 65535.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

Telnet to a Switch by specifying the IP address:

```
DES-3200-28P:admin#telnet 10.90.90.90
Command: telnet 10.90.90.90



                      DES-3200-28P Fast Ethernet Switch
                            Command Line Interface

                           Firmware: Build 4.03.004
           Copyright(C) 2012 D-Link Corporation. All rights reserved.
UserName:
```

Chapter 69 TFTP/FTP Client Command List

download [firmware_fromTFTP {<ipaddr> src_file <path_filename 64> {dest_file <pathname 64>} {boot_up}} | cfg_fromTFTP {<ipaddr> src_file <path_filename 64> {dest_file <pathname 64>}} | firmware_fromFTP [<ipaddr> {tcp_port <tcp_port_number1-65535>} src_file <path_filename 64> | ftp:<string user:password@ipaddr:tcpport/path_filename>] {dest_file <path_filename 64> {boot_up}} | cfg_fromFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} src_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {dest_file <path_filename 64>}]
upload [cfg_toTFTP {<ipaddr> dest_file <path_filename 64> {src_file <pathname 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}} | log_toTFTP{ <ipaddr> dest_file <path_filename 64>} | attack_log_toTFTP{ <ipaddr> dest_file <path_filename 64>} | firmware_toTFTP{ <ipaddr> dest_file <path_filename 64> {src_file <path_filename 64>}} | cfg_toFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {src_file<path_filename 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>} } {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] | attack_log_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] | firmware_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {src_file <pathname 64>}]
config tftp {server <ipaddr> | firmware_file <path_filename 64> | cfg_file <path_filename 64> | log_file <path_filename 64> | attack_log_file <path_filename 64> | certificate_file <path_filename 64> | key_file <path_filename 64> | tech_support_file <path_filename 64> | debug_error_log_file <path_filename 64> | sim_firmware_file <path_filename 64> | sim_cfg_file <path_filename 64> | sim_log_file <path_filename 64>}
show tftp

69-1 download

Description

This command is used to download the firmware image and configuration from TFTP/FTP server.

Format

download [firmware_fromTFTP {<ipaddr> src_file <path_filename 64> {dest_file <pathname 64>} {boot_up}} | cfg_fromTFTP {<ipaddr> src_file <path_filename 64> {dest_file <pathname 64>}} | firmware_fromFTP [<ipaddr> {tcp_port <tcp_port_number1-65535>} src_file <path_filename 64> | ftp:<string user:password@ipaddr:tcpport/path_filename>] {dest_file <path_filename 64> {boot_up}} | cfg_fromFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} src_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {dest_file <path_filename 64>}]

Parameters

firmware_fromTFTP – Specify to download firmware from a TFTP server. **<ipaddr>** - (Optional) The IP address of the TFTP server. **src_file** - (Optional) Used to identify the parameter “path_filename”. **<path_filename 64>** - Enter the source file path name here. This name can be up to 64 characters long. **dest_file** - (Optional) Used to identify the parameter “path_filename”. **<pathname 64>** - Enter the destination file path name here. **boot_up** – (Optional) Assign the downloaded file as boot-up image.
cfg_fromTFTP – Specify to download a configuration file from a TFTP server. **<ipaddr>** - (Optional) The IP address of the TFTP server. **src_file** - (Optional) Used to identify the parameter “path_filename”. **<path_filename 64>** - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long. **dest_file** - (Optional) Used to identify the parameter “path_filename”. **<pathname 64>**- The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up configuration file.
firmware_fromFTP – Specify to download firmware from a FTP server. **<ipaddr>** - (Optional) The IP address of the FTP server. **tcp_port** - Specify the TCP port. **<tcp_port_number1-65535>** - Enter a value between 1 and 65535. **src_file** - Specify the source file location. **<path_filename 64>** - The pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long. **ftp:** - Specify the FTP site. **<string user:password@ipaddr:tcpport/path_filename>** - Enter the FTP directory. **dest_file** – Used to identify the parameter “path_filename”. **<path_filename 64>** - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up configuration file. **boot_up** - (Optional) Assign the downloaded file as boot-up image.
cfg_fromFTP – Specify to download a configuration file from a FTP server. **<ipaddr>** - The IP address of the FTP server. **tcp_port** - (Optional) Specify the TCP port. **<tcp_port number 1-65535>** - Enter a value between 1 and 65535. **src_file** - Used to identify the parameter “path_filename”. **<path_filename 64>** - The pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long. **ftp:** - Specify the FTP site. **<string user:password@ipaddr:tcpport/path_filename>** - Enter the FTP directory. **dest_file** – Used to identify the parameter “path_filename”. **<path_filename 64>** - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up configuration file.

Restrictions

Only Administrator-level users can issue this command.

Example

To download firmware from TFTP:

```
DES-3200-28P:admin#download firmware_fromTFTP 10.54.71.1 src_file px.had
Command: download firmware_fromTFTP 10.54.71.1 src_file px.had

Connecting to server.................. Done.
Download firmware..................... Done.  Do not power off!
Please wait, programming flash......... Done.

DES-3200-28P:admin#
```

To download configuration from TFTP:

```
DES-3200-28P:admin#download cfg_fromTFTP 10.54.71.1 src_file cfg01.txt
Command: download cfg_fromTFTP 10.54.71.1 src_file cfg01.txt

Connecting to server..................…. Done.
Download configuration................. Done.

DES-3200-28P:admin#
```

69-2 upload

Description

This command is used to upload firmware and configuration from device to TFTP/FTP server.

Format

upload [cfg_toTFTP {<ipaddr> dest_file <path_filename 64> {src_file <pathname 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}} | log_toTFTP{ <ipaddr> dest_file <path_filename 64>} | attack_log_toTFTP{ <ipaddr> dest_file <path_filename 64>} | firmware_toTFTP{ <ipaddr> dest_file <path_filename 64> {src_file <path_filename 64>}} | cfg_toFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {src_file<path_filename 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>} } {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] | attack_log_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] | firmware_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {src_file <pathname 64>}]

Parameters

cfg_toTFTP – Specify that the configuration file will be uploaded to the TFTP server.
- **<ipaddr>** - The IP address of the TFTP server.
- **dest_file** - Used to identify the parameter “path_filename”.
  - **<path_filename 64>** - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters

long.

src_file - (Optional) Used to identify the parameter “path_filename”.

<pathname 64> - The pathname specifies an absolute pathname on the device file system.

include - (Optional) Specify to include lines that contain the specified filter string.

exclude - (Optional) Specify to exclude lines that contain the specified filter string.

begin - (Optional) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

include - (Optional) Specify to include lines that contain the specified filter string.

exclude - (Optional) Specify to exclude lines that contain the specified filter string.

begin - (Optional) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

include - (Optional) Specify to include lines that contain the specified filter string.

exclude - (Optional) Specify to exclude lines that contain the specified filter string.

begin - (Optional) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

---

log_toTFTP - Specify to upload a log file from device to TFTP server.

<ipaddr> - The IP address of the TFTP server.

dest_file - Used to identify the parameter “path_filename”.

<path_filename 64> - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

---

attack_log_toTFTP – Specify that the attack log will be uploaded to the TFTP server.

<ipaddr> - The IP address of the TFTP server.

dest_file - Used to identify the parameter “path_filename”.

<path_filename 64> - Specify the path name on the TFTP server to hold the attack log. This name can be up to 64 characters long.

---

firmware_toTFTP – Specify that the firmware file will be uploaded to the TFTP server.

<ipaddr> - The IP address of the TFTP server.

dest_file - Used to identify the parameter “path_filename”.

<path_filename 64> - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

src_file - (Optional) Used to identify the parameter “path_filename”.
<pathname 64> - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up image. This name can be up to 64 characters long.

cfg_toFTP – Specify that the configuration file will be uploaded to the FTP server.
<ipaddr> - The IP address of the FTP server.
tcp_port - Specify the TCP port.
<tcp_port_number1-65535> - Enter a value between 1 and 65535.
dest_file - Used to identify the parameter “path_filename”.
<path_filename 64> - The pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.
ftp: - Specify the FTP site.
<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.
src_file - (Optional) Used to identify the parameter “path_filename”.
<pathname 64> - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up CFG file.
include - (Optional) Specify to include lines that contain the specified filter string.
exclude - (Optional) Specify to exclude lines that contain the specified filter string.
begin - (Optional) The first line that contains the specified filter string will be the first line of the output.
<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
include - (Optional) Specify to include lines that contain the specified filter string.
exclude - (Optional) Specify to exclude lines that contain the specified filter string.
begin - (Optional) The first line that contains the specified filter string will be the first line of the output.
<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
include - (Optional) Specify to include lines that contain the specified filter string.
exclude - (Optional) Specify to exclude lines that contain the specified filter string.
begin - (Optional) The first line that contains the specified filter string will be the first line of the output.
<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

log_toFTP - Specify to upload a log file from device to FTP server.
<ipaddr> - The IP address of the FTP server.
tcp_port - Specify the TCP port.
<tcp_port_number1-65535> - Enter a value between 1 and 65535.

dest_file - Used to identify the parameter “path_filename”. **<path_filename 64>** - The pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long. **ftp:** - Specify the FTP site. <string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.
attack_log_toFTP – Specify that the attack log will be uploaded to the FTP server. **<ipaddr>** - The IP address of the FTP server. **tcp_port** - Specify the TCP port. **<tcp_port_number1-65535>** - Enter a value between 1 and 65535. **dest_file** - Used to identify the parameter “path_filename”. **<path_filename 64>** - Specify the path name on the FTP server to hold the attack log. This name can be up to 64 characters long. **ftp:** - Specify the FTP site. <string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.
firmware_toFTP – Specify that the firmware file will be uploaded to the FTP server. **<ipaddr>** - The IP address of the FTP server. **tcp_port** - Specify the TCP port. **<tcp_port_number1-65535>** - Enter a value between 1 and 65535. **dest_file** - Used to identify the parameter “path_filename”. **<path_filename 64>** - The pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long. **ftp:** - Specify the FTP site. **<string user:password@ipaddr:tcpport/path_filename>** - Enter the FTP directory. **src_file** - (Optional) Used to identify the parameter “path_filename”. **<pathname 64>** - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up image. This name can be up to 64 characters long.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To upload firmware from a file system device to a TFTP server:

```
DES-3200-28P:admin#upload firmware_toTFTP 10.90.90.10 dest_file d:\firmware.had

Command: upload firmware_toTFTP 10.90.90.10 dest_file d:\firmware.had

 Connecting to server.................. Done.
 Upload firmware...................... Done.
Success.

DES-3200-28P:admin#
```

To display a scenario where the uploading of the firmware to the TFTP server failed, because of an incorrect or missing filename from the source. This error can also be found if the directory, on the source, does not exit.

```
DES-3200-28P:admin#upload firmware_toTFTP 10.90.90.10 dest_file D:/firmware.had
src_file 4.00.020.had
Command: upload firmware_toTFTP 10.90.90.10 dest_file D:/firmware.had src_file
4.00.020.had

 No such file or directory.

Fail!

DES-3200-28P:admin#
```

To upload configuration from TFTP:

```
DES-3200-28P:admin#upload cfg_toTFTP 10.90.90.10 dest_file d:\config.cfg
Command: upload cfg_toTFTP 10.90.90.10 dest_file d:\config.cfg

 Connecting to server................... Done.
 Upload configuration.................. Done.
Success.

DES-3200-28P:admin#
```

To display a scenario where the uploading of the config file to the TFTP server failed, because of an incorrect or missing filename from the source. This error can also be found if the directory, on the source, does not exit.

```
DES-3200-28P:admin#upload cfg_toTFTP 10.90.90.10 dest_file d:\config.cfg
src_file missing.cfg
Command: upload cfg_toTFTP 10.90.90.10 dest_file d:\config.cfg src_file
missing.cfg

 No such file or directory.

Fail!

DES-3200-28P:admin#
```

To upload the attack log:

```
DES-3200-28P:admin#upload attack_log_toTFTP 10.90.90.10 dest_file d:\attack.txt
Command: upload attack_log_toTFTP 10.90.90.10 dest_file d:\attack.txt

Success.

DES-3200-28P:admin#
```

69-3 config tftp

Description

This command is used to pre-configure TFTP server and file pathname on the TFTP server.

Format

config tftp {server <ipaddr> | firmware_file <path_filename 64> | cfg_file <path_filename 64> | log_file <path_filename 64> | attack_log_file <path_filename 64> | certificate_file <path_filename 64> | key_file <path_filename 64> | tech_support_file <path_filename 64> | debug_error_log_file <path_filename 64> | sim_firmware_file <path_filename 64> | sim_cfg_file <path_filename 64> | sim_log_file <path_filename 64>}

Parameters

server - (Optional) Specify the IP address of the TFTP server. **<ipaddr>** - The IP address of the TFTP server.
firmware_file - (Optional) Specify the pathname supports “download/upload firmware_fromTFTP” function. **<path_filename 64>** - Specify the pathname supports “download/upload firmware_fromTFTP” function.
cfg_file - (Optional) Specify the pathname supports “download/upload cfg_fromTFTP” function. **<path_filename 64>** - Specify the pathname supports “download/upload cfg_fromTFTP” function.
log_file - (Optional) Specify the pathname supports “upload log_toTFTP” function. **<path_filename 64>** - Specify the pathname supports “upload log_toTFTP” function.
attack_log_file - (Optional) Specify the pathname supports “upload attack_log_toTFTP” function. **<path_filename 64>** - Specify the pathname supports “upload attack_log_toTFTP” function.
certificate_file - (Optional) Specify the pathname supports “download ssl certificate” function. **<path_filename 64>** - Specify the pathname supports “download ssl certificate” function.
key_file - (Optional) Specify the pathname supports “download ssl certificate” function. **<path_filename 64>** - Specify the pathname supports “download ssl certificate” function.
tech_support_file - (Optional) Specify specifying the pathname supports “upload tech_support_toTFTP” function. **<path_filename 64>** - Specify specifying the pathname supports “upload tech_support_toTFTP” function.
debug_error_log_file - (Optional) Specify the pathname supports “debug error_log” function. **<path_filename 64>** - Specify the pathname supports “debug error_log” function.
sim_firmware_file - (Optional) Specify the pathname supports “download/upload sim_ms firmware_fromTFTP” function. **<path_filename 64>** - Specify the pathname supports “download/upload sim_ms firmware_fromTFTP” function.
sim_cfg_file - (Optional) Specify the pathname supports “downloa/upload sim_ms configuration_fromTFTP” function. **<path_filename 64>** - Specify the pathname supports “downloa/upload sim_ms configuration_fromTFTP” function.
sim_log_file - (Optional) Specify the pathname supports “upload sim_ms log_toTFTP” function. **<path_filename 64>** - Specify the pathname supports “upload sim_ms log_toTFTP” function.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure TFTP server:

```
DES-3200-28P:admin#config tftp server 10.90.90.10
Command: config tftp server 10.90.90.10

Success.

DES-3200-28P:admin#
```

To configure TFTP server and specify the pre defined firmware file, log file:

```
DES-3200-28P:admin#config tftp server 10.90.90.1 firmware_file DES3200.had
cfg_file log_tmp
Command: config tftp server 10.90.90.1 firmware_file DES3200.had cfg_file
log_tmp

Success.

DES-3200-28P:admin#
```

69-4 show tftp

Description

This command is used to show the TFTP server and the file path pre-configured by administer.

Format

show tftp

Parameters

None.

Restrictions

None.

Example

To show TFTP settings, if pre-configure server IPv4 address, firmware_file and cfg_file only:

```
DES-3200-28P:admin#show tftp
Command: show tftp

 TFTP Server Settings
 IPv4 Address : 10.90.90.1

 File Type              Path_filename
 --------------------   ----------------------
 firmware_file          DES3200.had
 cfg_file               log_tmp
 log_file
 attack_log_file
 certificate_file
 key_file
 tech_support_file
 debug_error_log_file
 sim_firmware_file
 sim_cfg_file
 sim_log_file


DES-3200-28P:admin#
```

Chapter 70 Time and SNTP Command List

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
show sntp
enable sntp
disable sntp
config time <date ddmthyyyy> <time hh:mm:ss>
config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | 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

70-1 config sntp

Description

This command is used to change SNTP configurations.

Format

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}

Parameters

primary - (Optional) SNTP primary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
secondary - (Optional) SNTP secondary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
poll-interval - (Optional) Specify the polling interval range seconds. **<int 30-99999>** - Enter the polling interval range here. This value must be between 30 and 99999 seconds.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure SNTP:

```
DES-3200-28P:admin#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-
interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DES-3200-28P:admin#
```

70-2 show sntp

Description

This command is used to display SNTP current time source and configuration.

Format

show sntp

Parameters

None.

Restrictions

None.

Example

To show SNTP:

```
DES-3200-28P:admin#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

DES-3200-28P:admin#
```

70-3 enable sntp

Description

This command is used to turn on SNTP support.

Format

enable sntp

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable SNTP:

```
DES-3200-28P:admin#enable sntp
Command: enable sntp

Success.

DES-3200-28P:admin#
```

70-4 disable sntp

Description

This command is used to turn off SNTP support.

Format

disable sntp

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To disable SNTP:

```
DES-3200-28P:admin#disable sntp
Command: disable sntp

Success.

DES-3200-28P:admin#
```

70-5 config time

Description

This command is used to configure time and date settings of the device.

Format

config time <date ddmthyyyy> <time hh:mm:ss>

Parameters

<date ddmthyyyy> - Specify the system clock date. An example would look like this: '30jun2010'.
<time hh:mm:ss> - Specify the system clock time. An example would look like this: '12:00:00'.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure time:

```
DES-3200-28P:admin#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3200-28P:admin#
```

70-6 config time_zone

Description

This command is used to configure time zone of the device.

Format

config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}

Parameters

operator - (Optional) Specify the operator of time zone. **[+ | -]** - Specify that time should be added or subtracted to or from the GMT.
hour - (Optional) Specify the hour of time zone. **<gmt_hour 0-13>** - Enter the hour value of the time zone here. This value must be between 0 and 13.
min - (Optional) Specify the minute of time zone. **<minute 0-59>** - Enter the minute value of the time zone here. This value must be between 0 and 59.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure time_zone:

```
DES-3200-28P:admin#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3200-28P:admin#
```

70-7 config dst

Description

This command is used to configure Daylight Saving Time of the device.

Format

config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]

Parameters

disable - Disable the Daylight Saving Time of the Switch.

repeating - Set the Daylight Saving Time to repeating mode.

- **s_week, e_week** - (Optional) Configure the start /end week number of Daylight Saving Time.
  - **<start_week 1-4, last>** - Enter the starting week number of Daylight Saving Time here. This value must be between 1 and 4.
  - **<end_week 1-4, last>** - Enter the ending week number of Daylight Saving Time here. This value must be between 1 and 4.
- **s_day, e_day** - (Optional) Configure the start /end day number of Daylight Saving Time.
  - **<start_day sun-sat>** - Enter the starting day value of Daylight Saving Time here. This value must either be sun, mon, tue, wed, thu, fri or sat.
  - **<end_day sun-sat>** - Enter the ending day value of Daylight Saving Time here. This value must either be sun, mon, tue, wed, thu, fri or sat.
- **s_mth, e_mth** - (Optional) Configure the start /end month number of Daylight Saving Time.
  - **<start_mth 1-12>** - Enter the starting month number of Daylight Saving Time here. This value must be between 1 and 12.
  - **<end_mth 1-12>** - Enter the ending month number of Daylight Saving Time here. This value must be between 1 and 12.
- **s_time, e_time** - (Optional) Configure the start /end time of Daylight Saving Time.
  - **<start_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
  - **<end_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
- **offset** - (Optional) Indicates number of minutes to add or to subtract during summertime. The ranges of offset are 30, 60, 90,120. The default value is 60.
  - **30** - Specify that the offset range will 30 minutes.
  - **60** - Specify that the offset range will 60 minutes.
  - **90** - Specify that the offset range will 90 minutes.
  - **120** - Specify that the offset range will 120 minutes.

annual - Set the Daylight Saving Time to annual mode.
- **s_date, e_date** - (Optional) Configure the start /end date of Daylight Saving Time.
  - **<start_date 1-31>** - Enter the starting date of Daylight Saving Time here. This range must be between 1 an 31.
  - **<end_date 1-31>** - Enter the ending date of Daylight Saving Time here. This range must be between 1 an 31.
- **s_mth, e_mth** - (Optional) Configure the start /end month number of Daylight Saving Time.
  - **<start_mth 1-12>** - Enter the starting month number of Daylight Saving Time here. This value must be between 1 and 12.
  - **<end_mth 1-12>** - Enter the ending month number of Daylight Saving Time here. This value must be between 1 and 12.
- **s_time, e_time** - (Optional) Configure the start /end time of Daylight Saving Time.
  - **<start_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
  - **<end_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
- **offset** - (Optional) Indicates number of minutes to add or to subtract during summertime. The ranges of offset are 30, 60, 90,120; default value is 60.
  - **30** - Specify that the offset range will 30 minutes.
  - **60** - Specify that the offset range will 60 minutes.
  - **90** - Specify that the offset range will 90 minutes.
  - **120** - Specify that the offset range will 120 minutes.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure time:

```
DES-3200-28P:admin#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00
e_week
 2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e
_day wed e_mth 10 e_time 15:30 offset 30

Success.

DES-3200-28P:admin#
```

70-8 show time

Description

This command is used to display time states.

Format

show time

Parameters

None.

Restrictions

None.

Example

To show time:

```
DES-3200-28P:admin#show time
Command: show time

     Current Time Source  : System Clock
     Boot Time    : 9 May 2011  06:20:55
     Current Time : 9 May 2011  07:46:10
     Time Zone    : GMT +00:00
     Daylight Saving Time  : Disabled
         Offset In Minutes : 60
         Repeating    From : Apr 1st  Sun 00:00
                      To   : Oct last Sun 00:00
         Annual       From : 29 Apr 00:00
                      To   : 12 Oct 00:00

DES-3200-28P:admin#
```

Chapter 71 Trace Route Command List

traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}
traceroute6 <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

71-1 traceroute

Description

This command is used to trace the routed path between the Switch and a destination end station.

Format

traceroute <ipaddr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

Parameters

<ipaddr> - Specify the IP address of the destination end station.
ttl - (Optional) The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The traceroute command will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. **<value 1-60>** - Enter the time to live value here. This value must be between 1 and 60.
port - (Optional) The port number. The value range is from 30000 to 64900. **<value 30000-64900>** - Enter the port number here. This value must be between 30000 and 64900.
timeout - (Optional) Defines the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds. **<sec 1-65535>** - Enter the timeout period value here. This value must be between 1 and 65535 seconds.
probe - (Optional) The number of probing. The range is from 1 to 9. If unspecified, the default value is 1. **<value 1-9>** - Enter the probing number value here. This value must be between 1 and 9.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

Trace the routed path between the Switch and 10.48.74.121:

```
DES-3200-28P:admin#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

1   <10 ms.     10.12.73.254
2   <10 ms.     10.19.68.1
3   <10 ms.     10.48.74.121

Trace complete.
DES-3200-28P:admin#
```

71-2 traceroute6

Description

This command is used to trace the IPv6 routed path between the Switch and a destination end station.

Format

traceroute6 <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

Parameters

<ipv6addr> - Specify the IPv6 address of the destination end station.
ttl - (Optional) The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The traceroute command will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. **<value 1-60>** - Enter the time to live value here. This value must be between 1 and 60.
port - (Optional) The port number. The value range is from 30000 to 64900. **<value 30000-64900>** - Enter the port number here. This value must be between 30000 and 64900.
timeout - (Optional) Defines the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds. **<sec 1-65535>** - Enter the timeout period value here. This value must be between 1 and 65535 seconds.
probe - (Optional) The number of probing. The range is from 1 to 9. If unspecified, the default value is 1. **<value 1-9>** - Enter the probing number value here. This value must be between 1 and 9.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

Trace the IPv6 routed path between the Switch and 3000::1:

```
DES-3200-28P:admin#traceroute6 3000::1 probe 3
Command: traceroute6 3000::1 probe 3

1   <10 ms.     1345:142::11
2   <10 ms.     2011:14::100
3   <10 ms.     3000::1

Trace complete.
DES-3200-28P:admin#
```

Trace the IPv6 routed path between the Switch and 1210:100::11 with port 40000:

```
DES-3200-28P:admin#traceroute6 1210:100::11 port 40000
Command: traceroute6 1210:100::11 port 40000

1   <10 ms.     3100::25
2   <10 ms.     4130::100
3   <10 ms.     1210:100::11

Trace complete.
DES-3200-28P:admin#
```

Chapter 72 Traffic Control Command List

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] |unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}
config traffic trap [none | storm_occurred | storm_cleared | both]
show traffic control {<portlist>}
config traffic control log state [enable | disable]
config traffic control auto_recover_time [<min 0> | <min 1-65535>]

72-1 config traffic control

Description

This command is used to configure broadcast/ multicast/ unicast packet storm control. Shutdown mode is provided to monitor the traffic rate in addition to the storm control drop mode. If traffic rate is too high, this port will be shut down.

Format

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}

Parameters

<portlist> - Used to specify a range of ports to be configured. **all** - Specify that all the ports will be used for this configuration.
broadcast - (Optional) Enable or disable broadcast storm control. **enable** - Specify that broadcast storm control will be enabled. **disable** - Specify that broadcast storm control will be disabled.
multicast - (Optional) Enable or disable multicast storm control. **enable** - Specify that multicast storm control will be enabled. **disable** - Specify that multicast storm control will be disabled.
unicast - (Optional) Enable or disable unknown packet storm control. (Supported for drop mode only) **enable** - Specify that unicast storm control will be enabled. **disable** - Specify that unicast storm control will be disabled.
action - (Optional) One of the two options for action is specified for storm control, shutdown or drop mode. Shutdown mode is a function of software, drop mode is implemented by the chip. If shutdown mode is specified, it is necessary to configure values for the countdown and time_interval parameters. **drop** - Specify that the action applied will be drop mode. **shutdown** - Specify that the action applied will be shutdown mode.
threshold - (Optional) The upper threshold, at which point the specified storm control is triggered. The <value> is the number of broadcast/multicast packets per second received by the Switch that will trigger the storm traffic control measure. The threshold is expressed as PPS (packets per second) and must be an unsigned integer. **<value 0-255000>** - Enter the upper threshold value here. This value must be between 0 and 255000.

countdown - (Optional) Timer for shutdown mode. If a port enters the shutdown Rx state and this timer runs out, port will be shutdown forever. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter. **<min 0>** - 0 disables the forever state, meaning that the port will not enter the shutdown forever state. **<min 3-30>** - Enter the countdown timer value here. This value must be between 3 and 30. **disable** – Specify that the countdown timer will be disabled.
time_interval - (Optional) The sampling interval of received packet counts. The possible value will be m-n seconds. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter. **<sec 5-600>** - Enter the time interval value here. This value must be between 5 and 600.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To configure the parameters so that the traffic control status is enabled on ports 1-12:

```
DES-3200-28P:admin#config traffic control 1-12 broadcast enable action shutdown
threshold 1 countdown 5 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown threshold
1 countdown 5 time_interval 10

Success.

DES-3200-28P:admin#
```

72-2 config traffic trap

Description

This command is used to configure trap modes.

Occurred Mode: This trap is sent when a packet storm is detected by the packet storm mechanism.

Cleared Mode: This trap is sent when the packet storm is cleared by the packet storm mechanism.

Format

config traffic trap [none | storm_occurred | storm_cleared | both]

Parameters

none - No trap state is specified for storm control.
storm_occurred - Occurred mode is enabled and cleared mode is disabled.
storm_cleared - Occurred mode is disabled and cleared mode is enabled.
both - Both occurred and cleared modes are enabled.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To enable both the occurred mode and cleared mode traffic control traps:

```
DES-3200-28P:admin#config traffic trap both
Command: config traffic trap both

Success.

DES-3200-28P:admin#
```

72-3 show traffic control

Description

This command is used to display the current traffic control settings.

Format

show traffic control {<portlist>}

Parameters

<portlist> - (Optional) Used to specify the range of ports to be shown.
If no parameter is specified, the system will display the packet storm control configuration for all ports.

Restrictions

None.

Example

To display the traffic control parameters for ports 1 to 10:

```
DES-3200-28P:admin#show traffic control  1-10
Command: show traffic control 1-10


Traffic Control Trap             : [Both]
Traffic Control Log              : Enabled
Traffic Control Auto Recover Time: 0 Minutes

Port Thres  Broadcast Multicast Unicast  Action   Count    Time     Shutdown
     hold   Storm     Storm     Storm              down     Interval Forever
---- ------ --------- --------- -------- -------- -------- -------- --------
1    1      Enabled   Disabled  Disabled shutdown 5        10
2    1      Enabled   Disabled  Disabled shutdown 5        10
3    1      Enabled   Disabled  Disabled shutdown 5        10
4    1      Enabled   Disabled  Disabled shutdown 5        10
5    1      Enabled   Disabled  Disabled shutdown 5        10
6    1      Enabled   Disabled  Disabled shutdown 5        10
7    1      Enabled   Disabled  Disabled shutdown 5        10
8    1      Enabled   Disabled  Disabled shutdown 5        10
9    1      Enabled   Disabled  Disabled shutdown 5        10
10   1      Enabled   Disabled  Disabled shutdown 5        10

DES-3200-28P:admin#
```

72-4 config traffic control log state

Description

This command is used to configure the traffic control log state. When the log state is enabled, traffic control states are logged when a storm occurs and when a storm is cleared. If the log state is disabled, traffic control events are not logged.

Note: The log state is only applicable for shutdown mode. Since shutdown mode only support broadcast and multicast storm control, doesn't support unicast storm control. The log only generate for broadcast and multicast storm control.

Format

config traffic control log state [enable | disable]

Parameters

enable - Both occurred and cleared are logged. **disable** - Neither occurred nor cleared is logged.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To configure the traffic log state on the Switch:

```
DES-3200-28P:admin#config traffic control log state enable
Command: config traffic control log state enable

Success.

DES-3200-28P:admin#
```

72-5 config traffic control auto_recover_time

Description

This command is used to configure the traffic auto recover time that allowed for a port to recover from shutdown forever status.

Format

config traffic control auto_recover_time [<min 0> | <min 1-65535>]

Parameters

auto_recover_time - The time allowed for auto recovery from shutdown for a port. The default value is 0, so no auto recovery is possible; the port remains in shutdown forever mode. This requires manual entry of the CLI command “config ports [<portlist> | all] state enable" to return the port to a forwarding state. The default value is 0, which means disable auto recover mode, shutdown forever.
<min 0> - Specify that the auto recovery time will be disabled.
<min 1-65535> - Enter the auto recovery time value here. This value must be between 1 and 65535.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To configure the auto recover time to 5 minutes:

```
DES-3200-28P:admin#config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DES-3200-28P:admin#
```

Chapter 73 Traffic Segmentation Command List

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation {<portlist>}

73-1 config traffic_segmentation

Description

This command is used to configure the traffic segmentation.

Format

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]

Parameters

<portlist> - Specify a range of ports to be configured. **all -** Specify that all the ports will be used for this configuration.
forward_list - Specify a range of port forwarding domain. **null** - Specify a range of port forwarding domain is null. **all** – Specify all ports to be configured. **<portlist>** - Specify a range of ports to be configured.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To configure traffic segmentation:

```
DES-3200-28P:admin#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DES-3200-28P:admin#
```

73-2 show traffic_segmentation

Description

This command is used to display current traffic segmentation table.

Format

show traffic_segmentation {<portlist>}

Parameters

<portlist> - (Optional) Specify a range of ports to be displayed.
If no parameter is specified, the system will display all current traffic segmentation tables.

Restrictions

None.

Example

To display traffic segmentation table:

```
DES-3200-28P:admin#show traffic_segmentation 1-10
Command: show traffic_segmentation 1-10

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------------------------------
1      11-15
2      11-15
3      11-15
4      11-15
5      11-15
6      11-15
7      11-15
8      11-15
9      11-15
10     11-15


DES-3200-28P:admin#
```

Chapter 74 Trusted Host Command List

create trusted_host [<ipaddr> | network <network_address>] {snmp | telnet | ssh | http | https | ping}
delete trusted_host [ipaddr <ipaddr> | network <network_address> | all]
config trusted_host [<ipaddr> | network <network_address>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}
show trusted_host

74-1 create trusted_host

Description

This command is used to create the trusted host. The switch allows you to specify up to ten IP addresses that are allowed to manage the Switch via in-band SNMP or TELNET based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.

When the access interface is not specified, the trusted host will be created for all interfaces.

Format

create trusted_host [<ipaddr> | network <network_address>] {snmp | telnet | ssh | http | https | ping}

Parameters

<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. **<network_address>** - Enter the network address used here.
snmp - (Optional) Specify trusted host for SNMP.
telnet - (Optional) Specify trusted host for TELENT.
ssh - (Optional) Specify trusted host for SSH.
http - (Optional) Specify trusted host for HTTP.
https - (Optional) Specify trusted host for HTTPs.
ping - (Optional) Specify trusted host for PING.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To create the trusted host:

```
DES-3200-28P:admin#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DES-3200-28P:admin#
```

74-2 delete trusted_host

Description

This command is used to delete a trusted host entry made using the create trusted_host command above.

Format

delete trusted_host [ipaddr <ipaddr> | network <network_address> | all]

Parameters

ipaddr - The IP address of the trusted host. **<ipaddr>** - Enter the IP address used for this configuration here.
network - The network address of the trusted network. **<network_address>** - Enter the network address used for this configuration here.
all - All trusted hosts will be deleted.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To delete the trusted host:

```
DES-3200-28P:admin#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

DES-3200-28P:admin#
```

74-3 config trusted_host

Description

This command is used to configure the access interfaces for the trusted host.

Format

config trusted_host [<ipaddr> | network <network_address>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}

Parameters

<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. **<network_address>** - Enter the network address used here.
add - Add interfaces for that trusted host.
delete - Delete interfaces for that trusted host.
snmp - (Optional) Specify trusted host for SNMP.
telnet - (Optional) Specify trusted host for TELENT.
ssh - (Optional) Specify trusted host for SSH.
http - (Optional) Specify trusted host for HTTP.
https - (Optional) Specify trusted host for HTTPs.
ping - (Optional) Specify trusted host for PING.
all – (Optional) Specify trusted host for all application.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure the trusted host:

```
DES-3200-28P:admin#config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

DES-3200-28P:admin#
```

74-4 show trusted_host

Description

This command is used to display a list of trusted hosts entered on the Switch using the create trusted_host command above.

Format

show trusted_host

Parameters

None.

Restrictions

None.

Example

To display trusted host:

```
DES-3200-28P:admin#show trusted_host
Command: show trusted_host


Management Stations

IP Address                                  Access Interface
-------------------------------------------------------------------
10.48.74.121                                SNMP Telnet SSH HTTP HTTPs Ping

Total Entries: 1


DES-3200-28P:admin#
```

Chapter 75 Unicast Routing Command List

create iproute [default] <ipaddr> {<metric 1-65535>}
delete iproute [default]
show iproute {<network_address>} {static}

75-1 create iproute

Description

This command is used to create an IP static route.

Format

create iproute [default] <ipaddr> {<metric 1-65535>}

Parameters

default - Create an IP default route (0.0.0.0/0).
<ipaddr> - The IP address for the next hop router.
<metric 1-65535> - (Optional) Enter the metric value here. This value must be between 1 and 65535. The default setting is 1.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To add an IP default route:

```
DES-3200-28P:admin#create iproute default 10.1.1.254
Command: create iproute default 10.1.1.254

Success.

DES-3200-28P:admin#
```

75-2 delete iproute

Description

This command is used to delete an IP route entry from the Switch's IP routing table.

Format

delete iproute [default]

Parameters

default - Deletes an IP default route (0.0.0.0/0).

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To delete an IP default route:

```
DES-3200-28P:admin#delete iproute default 10.1.1.254
Command: delete iproute default 10.1.1.254

Success.

DES-3200-28P:admin#
```

75-3 show iproute

Description

This command is used to display the Switch's current IP routing table.

Format

show iproute {<network_address>} {static}

Parameters

<network_address> - (Optional) Specify the destination network address of the route to be displayed.
static - (Optional) Specify to display only static routes. One static route may be active or inactive.

Restrictions

None.

Example

To display the contents of the IP routing table:

```
DES-3200-28P:admin#show iproute
Command: show iproute


Routing Table

IP Address/Netmask  Gateway          Interface       Cost      Protocol
------------------  ---------------  ------------  --------  --------
10.1.1.0/24         0.0.0.0          System        1         Local
192.168.1.0/24      0.0.0.0          ip1           1         Local

Total Entries : 2

DES-3200-28P:admin#
```

Chapter 76 VLAN Trunking Command List

enable vlan_trunk
disable vlan_trunk
config vlan_trunk ports [<portlist> | all] | state [enable | disable]
show vlan_trunk

76-1 enable vlan_trunk

Description

This command is used to enable the VLAN trunk function. When the VLAN trunk function is enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.

Format

enable vlan_trunk

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the VLAN Trunk:

```
DES-3200-28P:admin#enable vlan_trunk
Command: enable vlan_trunk

Success.

DES-3200-28P:admin#
```

76-2 disable vlan_trunk

Description

This command is used to disable the VLAN trunk function.

Format

disable vlan_trunk

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the VLAN Trunk:

```
DES-3200-28P:admin#disable vlan_trunk
Command: disable vlan_trunk

Success.

DES-3200-28P:admin#
```

76-3 config vlan_trunk

Description

This command is used to configure a port as a VLAN trunk port. By default, none of the port is a VLAN trunk port.

If the user enables the global VLAN trunk function and configurethe VLAN trunk ports, then the trunk port will be member port of all VLANs. That is, if a VLAN is already configured by the user, but the trunk port is not member port of that VLAN, this trunk port will atutomatically become tagged member port of that VLAN. If a VLAN is not created yet, the VLAN will be automatically created, and the trunk port will become tagged member of this VLAN.

When the user disables the VLAN trunk globally, all VLANs automatically created by VLAN Trunk enabled shall be destroyed, and all the automatically added port membership will be removed.

A VLAN trunk port and a non-VLAN trunk port cannot be grouped as an aggregated link. To change the VLAN trunk setting for an aggregated link, the user must apply the command to the master port. However, this setting will disappear as the aggregated link is destroyed, and the VLAN trunk setting of the individual port will follow the original setting of the port.

If the command is applied to link aggregation member port excluding the master, the command will be rejected.

The ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as VLAN trunk port, they are allowed to form an aggregated link.

For a VLAN trunk port, the VLANs on which the packets can be by passed will not be advertised by GVRP on this port. However, since the traffic on these VLANs are forwarded, this vlan trunk port should participate the MSTP instances corresponding to these VLAN.

Format

config vlan_trunk ports [<portlist> | all] | state [enable | disable]

Parameters

<portlist> - Enter a list of ports used for the configuration here. **all** - Specify that all the ports will be used for this configuration.
state - Specify that the port is a VLAN trunk port or not. **enable** - Specify that the port is a VLAN trunk port. **disable** - Specify that the port is not a VLAN trunk port.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure VLAN trunk ports:

```
DES-3200-28P:admin#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DES-3200-28P:admin#
```

Port 6 is LA-1 member port; port 7 is LA-2 master port:

```
DES-3200-28P:admin#config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DES-3200-28P:admin#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DES-3200-28P:admin#config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DES-3200-28P:admin#
```

Port 6 is LA-1 member port; port 7 is LA-1 master port:

```
DES-3200-28P:admin#config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DES-3200-28P:admin#
```

Port 6, 7 have different VLAN configurations before enabling VLAN trunk.

Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DES-3200-28P:admin#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DES-3200-28P:admin#
```

Port 6, 7 have the same VLAN configuration before enabling VLAN trunk.

Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DES-3200-28P:admin#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DES-3200-28P:admin#config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DES-3200-28P:admin#
```

76-4 show vlan_trunk

Description

This command is used to show the VLAN trunk configuration.

Format

show vlan_trunk

Parameters

None.

Restrictions

None.

Example

To show the VLAN Trunk information:

```
DES-3200-28P:admin#show vlan_trunk
Command: show vlan_trunk


VLAN Trunk Global Setting
----------------------------
VLAN Trunk Status  : Disabled
VLAN Trunk Member Ports : 1-5


DES-3200-28P:admin#
```

The following example displays the VLAN information which will also display VLAN trunk setting:

```
DES-3200-28P:admin#show vlan
Command: show vlan


VLAN Trunk State        : Enabled
VLAN Trunk Member Ports : 1-5


VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-28
Static Ports    : 1-28
Current Tagged Ports  :
Current Untagged Ports: 1-28
Static Tagged Ports   :
Static Untagged Ports : 1-28
Forbidden Ports       :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0


DES-3200-28P:admin#
```

Chapter 77 Password Recovery Command List

enable password_recovery
disable password_recovery
show password_recovery

77-1 enable password_recovery

Description

This command is used to enable the password recovery mode.

Format

enable password_recovery

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the password recovery mode:

```
DES-3200-28P:admin#enable password_recovery
Command: enable password_recovery

Success.

DES-3200-28P:admin#
```

77-2 disable password_recovery

Description

This command is used to disable the password recovery mode.

Format

disable password_recovery

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the password recovery mode:

```
DES-3200-28P:admin#disable password_recovery
Command: disable password_recovery

Success.

DES-3200-28P:admin#
```

77-3 show password_recovery

Description

This command is used to display the password recovery state.

Format

show password_recovery

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the password recovery state:

```
DES-3200-28P:admin#show password_recovery
Command: show password_recovery

 Running Configuration  : Enabled
 NV-RAM Configuration   : Enabled

DES-3200-28P:admin#
```

Appendix A Password Recovery Procedure

This chapter describes the procedure for resetting passwords on D-Link switches. Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This chapter explains how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the Switch.
2. Power on the Switch. After the 'Starting runtime image' message, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the "Password Recovery Mode." Once the Switch enters the "Password Recovery Mode," all ports on the Switch will be disabled and all port LEDs will be lit.

```
Boot Procedure                                          V4.00.001
--------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address   : 00-01-02-03-04-00
  H/W Version   : C1

  Please Wait, Loading V4.03.004 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
```

```
Password Recovery Mode
>
```

3. In the "Password Recovery Mode" only the following commands can be used.

Command	Parameters
reset config {force_agree}	The **reset config** command resets the whole configuration back to the default values. If **force_agree** is specified, the configuration will reset to default without the user's agreement.
reboot	The **reboot** command exits the Reset Password Recovery Mode and restarts the Switch. A confirmation message will be displayed to allow the user to save the current settings.

Command	Parameters
reset account	The **reset** account command deletes all the previously created accounts.
reset password {<username>}	The **reset password** command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The **show account** command displays all previously created accounts.

Appendix B System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity
system	System started up	System started up	Critical
	System warm start	System warm start	Critical
	System cold start	System cold start	Critical
	Configuration saved to flash	Configuration saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational
	System log saved to flash	System log saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational
	Configuration and log saved to flash	Configuration and log saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational
	Internal Power failed	Internal Power failed	Critical
	Internal Power is recovered	Internal Power is recovered	Critical
	Redundant Power failed	Redundant Power failed	Critical
	Redundant Power is working	Redundant Power is working	Critical
	Side Fan failed	Side Fan failed	Critical
	Side Fan recovered	Side Fan recovered	Critical
	Back Fan failed	Back Fan failed	Critical
	Back Fan recovered	Back Fan recovered	Critical
	Temperature sensor enters alarm state	Temperature sensor <sensorID> enters alarm state (current temperature: <temperature>)	Warning
	Temperature recovers to normal	Temperature sensor <sensorID> recovers to normal state (current temperature: <temperature>)	Informational
up/down-load	Firmware upgraded successfully	Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>)	Informational
	Firmware upgrade was unsuccessful	Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Configuration successfully downloaded	Configuration successfully downloaded by console(Username: <username>, IP: <ipaddr>)	Informational
	Configuration download was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Configuration successfully uploaded	Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational
	Configuration upload was unsuccessful	Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Log message successfully uploaded	Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational
	Log message upload was	Log message upload by console was	Warning

	unsuccessful	unsuccessful! (Username: <username>, IP: <ipaddr>)	
	Firmware successfully uploaded	Firmware successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational
	Firmware upload was unsuccessful	Firmware upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
Interface	Port link up	Port <portNum> link up, <link state>	Informational
	Port link down	Port <portNum> link down	Informational
Console	Successful login through Console	Successful login through Console (Username: <username>)	Informational
	Login failed through Console	Login failed through Console (Username: <username>)	Warning
	Logout through Console	Logout through Console (Username: <username>)	Informational
	Console session timed out	Console session timed out (Username: <username>)	Informational
Web	Successful login through Web	Successful login through Web (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>)	Warning
	Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>,)	Informational
	Web session timed out	Web session timed out (Username: <username>, IP: <ipaddr>,)	Informational
	Successful login through Web(SSL)	Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>,)	Informational
	Login failed through Web(SSL)	Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>,)	Warning
	Logout through Web(SSL)	Logout through Web(SSL) (Username: <username>, IP: <ipaddr>,)	Informational
	Web(SSL) session timed out	Web(SSL) session timed out (Username: <username>, IP: <ipaddr>,)	Informational
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>,)	Informational
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>,)	Warning
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>,)	Informational
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>,)	Informational
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational
STP	Topology changed	Topology changed (Instance:<InstanceID>, Port:<portNum>,MAC:<macaddr>)	notice
	Enable spanning tree protocol	Spanning Tree Protocol is enabled	Informational
	Disable spanning tree protocol	Spanning Tree Protocol is disabled	Informational
	New root bridge	CIST New Root bridge selected (MAC: <macaddr> Priority :<value>)	Informational

	New root bridge	CIST Region New Root bridge selected (MAC: <macaddr> Priority :<value>)	Informational
	New root bridge	MSTI Region New Root bridge selected (Instance:<InstanceID>, MAC: <macaddr> Priority :<value>)	Informational
	New root bridge	New Root bridge selected (MAC: <macaddr> Priority :<value>)	Informational
	New root port	New root port selected (Instance:<InstanceID>, Port:<portNum>)	notice
	Spanning Tree port status changed	Spanning Tree port status changed (Instance:<InstanceID>, Port:<portNum>) <old_status> -> <new_status>	notice
	Spanning Tree port role changed	Spanning Tree port role changed (Instance:<InstanceID>, Port:<portNum>) <old_role> -> <new_role>	Informational
	Spannnig Tree instance created	Spanning Tree instance created (Instance:<InstanceID>)	Informational
	Spannnig Tree instance deleted	Spanning Tree instance deleted (Instance:<InstanceID>)	Informational
	Spanning Tree Version changed	Spanning Tree version changed (new version:<new_version>)	Informational
	Spanning Tree MST configuration ID name and revision level changed	Spanning Tree MST configuration ID name and revision level changed (name:<name> ,revision level <revision_level>)	Informational
	Spanning Tree MST configuration ID VLAN mapping table added	Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>])	Informational
	Spanning Tree MST configuration ID VLAN mapping table deleted	Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>])	Informational
DoS	Spoofing attack 1. The soure ip is same as switch's interface ip but the source mac is different 2. Source ip is the same as the switch's IP in ARP packet 3. Self IP packet dected	Possible spoofing attack from (IP: <ipaddr> MAC: <macaddr> Port: <portNum>)	Critical
	The DoS attack is blocked	<dos_name> is blocked from (IP: <ipaddr> Port: <portNum>)	Critical
SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>)	Informational
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>,)	Warning
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational
	SSH server is enabled	SSH server is enabled	Informational
	SSH server is disabled	SSH server is disabled	Informational
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational

	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Web authenticated by AAA local method	Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web(SSL) authenticated by AAA local method	Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Web(SSL) authenticated by AAA local method	Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>,)	Informational
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Web(SSL) authenticated by AAA none method	Successful login through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none (Username: <username>)	Informational
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning

	Login failed through Console due to AAA server timeout or improper configuration	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Web authenticated by AAA server	Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through Web due to AAA server timeout or improper configuration	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful login through Web(SSL) authenticated by AAA server	Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Web(SSL) authenticated by AAA server	Login failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through Web(SSL) due to AAA server timeout or improper configuration	Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful login through Telnet authenticated by AAA server	Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through Telnet authenticated by AAA server	Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through Telnet due to AAA server timeout or improper configuration	Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful login through SSH authenticated by AAA server	Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Login failed through SSH authenticated by AAA server	Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Login failed through SSH due to AAA server timeout or improper configuration	Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through Console authenticated by AAA local_enable method	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Web authenticated by AAA local_enable method	Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Web authenticated by AAA local_enable method	Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning

	Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>,)	Informational
	Enable Admin failed through Web(SSL) authenticated by AAA local_enable method	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Telnet authenticated by AAA local_enable method	Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through SSH authenticated by AAA local_enable method	Successful Enable Admin through SSH from <userIP> authenticated by AAA local (Username: <username>)	Informational
	Enable Admin failed through SSH authenticated by AAA local_enable method	Enable Admin failed through <Telnet or Web or SSH> from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Web authenticated by AAA none method	Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Web(SSL) authenticated by AAA none method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Telnet authenticated by AAA none method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through SSH authenticated by AAA none method	Successful Enable Admin through SSH from <userIP> authenticated by AAA none (Username: <username>)	Informational
	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through Console due to AAA server timeout or improper configuration	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through	Enable Admin failed through Web from <userIP>	Warning

	Web due to AAA server timeout or improper configuration	due to AAA server timeout or improper configuration (Username: <username>)	
	Successful Enable Admin through Web(SSL) authenticated by AAA server	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Web(SSL) authenticated by AAA server	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through Web(SSL) due to AAA server timeout or improper configuration	Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through Telnet due to AAA server timeout or improper configuration	Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational
	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	AAA server timed out	AAA server <serverIP> (Protocol: <protocol>) connection failed	Warning
	AAA server ACK error	AAA server <serverIP> (Protocol: <protocol>) response is wrong	Warning
	AAA does not support this functionality	AAA doesn't support this functionality	Informational
Port security	port security is exceeded to its maximum learning size and will not learn any new address	Port security violation (MAC address:<macaddr> on port:<portNum>)	Warning
IMPB	Unauthenticated IP address encountered and discarded by ip IP-MAC port binding	Unauthenticated IP-MAC address and discarded by IMPB (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry is conflict with static ARP	Dynamic IMPB entry conflicts with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry is conflict with static FDB	Dynamic IMPB entry conflicts with static FDB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry conflicts with static IMPB	Dynamic IMPB entry conflicts with static IMPB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning

	Creating IMPB entry failed due to no ACL rule available	Creating IMPB entry failed due to no ACL rule being available(IP:<ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
IP and Password Changed	IP Address change activity	Management IP address was changed by (Username: <username>,IP:<ipaddr>)	Informational
	Password change activity	Password was changed by (Username: <username>,IP:<ipaddr>)	Informational
Safeguard Engine	Safeguard Engine is in normal mode	Safeguard Engine enters NORMAL mode	Informational
	Safeguard Engine is in filtering packet mode	Safeguard Engine enters EXHAUSTED mode	Warning
Packet Storm	Broadcast strom occurrence	Port <portNum> Broadcast storm is occurring	Warning
	Broadcast storm cleared	Port <portNum> Broadcast storm has cleared	Informational
	Multicast storm occurrence	Port <portNum> Multicast storm is occurring	Warning
	Multicast storm cleared	Port <portNum> Multicast storm has cleared	Informational
	Port shut down due to a packet storm	Port <portNum> is currently shut down due to a packet storm	Warning
Loop Back Dection	Port loop occurred	Port <portNum> LBD loop occurred. Port blocked.	Critical
	Port loop detection restarted after interval time	Port <portNum> LBD port recovered. Loop detection restarted.	Informational
	Port with VID loop occurred	Port <portNum> VID <vlanID> LBD loop occurred. Packet discard begun.	Critical
	Port with VID Loop detection restarted after interval time	Port <portNum> VID <vlanID> LBD recovered. Loop detection restarted.	Informational
802.1x	VID assigned from radius server after radius client authenticated by radius server successfully .This VID will assign to the port and this port will be the vlan untag port member.	Radius server <ipaddr> assigned vid :<vlanID> to port <portNum> (account :<username>)	Informational
	Ingress bandwidth assigned from radius server after radius client authenticated by radius server successfully .This Ingress bandwidth will assign to the port.	Radius server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <portNum> (account : <username>)	Informational
	Egress bandwidth assigned from radius server after radius client authenticated by radius server successfully .This egress bandwidth will assign to the port.	Radius server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <portNum> (account: <username>)	Informational
	802.1p default priority assigned from radius server after radius client authenticated by radius server successfully.This 802.1p default priority will assign to the port.	Radius server <ipaddr> assigned 802.1p deafult priority:<priority> to port <portNum> (account : <username>)	Informational

	802.1x Authentication failure	802.1x Authentication failure from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication success	802.1x Authentication success [for <reason>] from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Informational
CFM	Cross-connect is detected	CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)	Critical
	Error CFM CCM packet is detected	CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)	Warning
	Can not receive remote MEP's CCM packet	CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)	Warning
	Remote MEP's MAC reports an error status	CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)	Warning
	Remote MEP detects CFM defects	CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)	Informational
ARP	Gratuituios ARP detected duplicate IP.	Conflict IP was detected with this device ! (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: <ipif_name>).	Warning
DHCP	Detect untrusted DHCP server IP address	Detected untrusted DHCP server(IP: <ipaddr>, Port: <portNum>)	Informational
COMMAND LOGGING	Command Logging	<username>: execute command "<string>"	Informational
MBAC	A host passes the authentication	MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational
	A host fails to pass the authentication	MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <portNum>, VID: <vid>)	Critical
	A host is aged out	MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational
	The authorized user number on a port reaches the maximum user limit	Port <portNum> enters MAC-based Access Control stop learning state	Warning
	The authorized user number on a port is below the maximum user limit in a time interval (interval is project depended)	Port <portNum> recovers from MAC-based Access Control stop learning state	Warning
	The authorized user number on whole device reaches the maximum user limit	MAC-based Access Control enters stop learning state	Warning
	The authorized user number on whole device is below the maximum user limit in a time interval (interval is project	MAC-based Access Control recovers from stop learning state	Warning

	depended)		
BPDU Protection	BPDU attack happened	Port <port> enter BPDU under protection state (mode: drop)	Informational
	BPDU attack happened	Port <port> enter BPDU under protection state (mode: block)	Informational
	BPDU attack happened	Port <port> enter BPDU under protection state (mode: shutdown)	Informational
	BPDU attack automatically recover	Port <port> recover from BPDU under protection state automatically	Informational
	BPDU attack manually recover	Port <port> recover from BPDU under protection state manually	Informational
	System re-start reason: system fatal error	System re-start reason: system fatal error	Emergent
	System re-start reason: CPU exception	System re-start reason: CPU exception	Emergent
Diagnostic	Diagnostic: Burn in start	Diagnostic: Burn in start at %S	Informational
	Diagnostic: Burn in end	Diagnostic: Burn in end at %S	Informational
	Diagnostic: Burn in result	Diagnostic: Burn in result is %S	Informational
DULD	A unidirectional link has been detected on this port	Port: <portNum> is unidirectional	Informational
ERPS	Signal failure detected	Signal failure detected on node (MAC: <macaddr>)	Notice
	Signal failure cleared	Signal failure cleared on node (MAC: <macaddr>)	Notice
	RPL owner conflict.	RPL owner conflicted on the ring (MAC: <macaddr>)	Warning

Appendix C Trap Log Entries

This table lists the trap logs found on the Switch.

Trap Name	Variable Bind	Format	MIB Name
coldStart	None	V1/v2	SNMPv2-MIB
warmStart	None	V1/V2	SNMPv2-MIB
linkDown	ifIndex	V1/V2	IF-MIB
linkUp	ifIndex	V1/V2	IF-MIB
authenticationFailure	None	V1/V2	SNMPv2-MIB
newRoot	None	V1/V2	BRIDGE-MIB
topologyChange	None	V1/V2	BRIDGE-MIB
risingAlarm	alarmIndex, alarmVariable alarmSampleType, alarmValue, alarmRisingThreshold	V1/V2	RMON-MIB
fallingAlarm	alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmFallingThreshold	V1/V2	RMON-MIB
lldpRemTablesChange	lldpStatsRemTablesInserts lldpStatsRemTablesDeletes lldpStatsRemTablesDrops lldpStatsRemTablesAgeouts	V1/V2	LLDP-MIB
swPowerStatusChg	swPowerUnitIndex, swPowerID, swPowerStatus	V2	Equipment.MIB
swPowerFailure	swPowerUnitIndex, swPowerID, swPowerStatus	V2	Equipment.MIB
swPowerRecover	swPowerUnitIndex, swPowerID, swPowerStatus	V2	Equipment.MIB
swFanFailure	swFanUnitIndex swFanID	V2	Equipment.MIB

swFanRecover	swFanUnitIndex swFanID	V2	Equipment.MIB
swHighTemperature	swTemperatureUnitIndex swTemperatureCurrent	V2	Equipment.MIB
swHighTemperatureRecover	swTemperatureUnitIndex swTemperatureCurrent	V2	Equipment.MIB
swLowTemperature	swTemperatureUnitIndex swTemperatureCurrent	V2	Equipment.MIB
swLowTemperatureRecover	swTemperatureUnitIndex swTemperatureCurrent	V2	Equipment.MIB
swPktStormOccurred	swPktStormCtrlPortIndex	V2	PktStormCtrl.mib
swPktStormCleared	swPktStormCtrlPortIndex	V2	PktStormCtrl.mib
swPktStormDisablePort	swPktStormCtrlPortIndex	V2	PktStormCtrl.mib
swSafeGuardChgToExhausted	swSafeGuardCurrentStatus	V2	SafeGuard.mib
swSafeGuardChgToNormal	swSafeGuardCurrentStatus	V2	SafeGuard.mib
swIpMacBindingRecoverLearningTrap	swIpMacBindingPortIndex	V2	IPMacBind.mib
SwMacBasedAuthLoggedSuccess	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	mba.mib
swMacBasedAuthLoggedFail	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	mba.mib
SwMacBasedAuthAgesOut	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	mba.mib
swFilterDetectedTrap	swFilterDetectedIP swFilterDetectedport	V2	Filter.MIB
swPortLoopOccurred	swLoopDetectPortIndex	V2	LBD.mib
swPortLoopRestart	swLoopDetectPortIndex	V2	LBD.mib
swVlanLoopOccurred	swLoopDetectPortIndex	V2	LBD.mib
swVlanLoopRestart	swLoopDetectPortIndex	V2	LBD.mib

	swVlanLoopDetectVID		
swDdmAlarmTrap	swDdmPort swDdmThresholdType swDdmThresholdExceedType	V2	DDM.MIB
swDdmWarningTrap	swDdmPort swDdmThresholdType swDdmThresholdExceedType	V2	DDM.MIB
swBpduProtectionUnderAttackingTrap	swBpduProtectionPortIndex swBpduProtectionPortMode	V2	BPDUProtection .MIB
swBpduProtectionRecoveryTrap	swBpduProtectionPortIndex swBpduProtectionRecoveryMethod	V2	BPDUProtection .MIB
swL2macNotification	swL2macNotifyInfo	V2	L2MGMT-MIB
swL2PortSecurityViolationTrap	swPortSecPortIndex swL2PortSecurityViolationMac	V2	L2MGMT-MIB
swERPSSFDetectedTrap	swERPSNodeId	V2	ERPS.mib
swERPSSFClearedTrap	swERPSNodeId	V2	ERPS.mib
swERPSRPLOwnerConflictTrap	swERPSNodeId	V2	ERPS.mib
agentCfgOperCompleteTrap	unitID agentCfgOperate agentLoginUserName	V2	Genmgmt.mib
agentFirmwareUpgrade	swMultiImageVersion	V2	Genmgmt.mib
agentGratuitousARPTrap	agentGratuitousARPIpAddr agentGratuitousARPMacAddr agentGratuitousARPPortNumber agentGratuitousARPInterfaceName	V2	Genmgmt.MIB
swSingleIPMSLinkDown	1: swSingleIPMSID 2: swSingleIPMSMacAddr 3: ifIndex	V2	SingleIP.mib
swSingleIPMSLinkUp	1: swSingleIPMSID 2: swSingleIPMSMacAddr 3: ifIndex	V2	SingleIP.mib
swSingleIPMSAuthFail	1: swSingleIPMSID 2: swSingleIPMSMacAddr	V2	SingleIP.mib
swSingleIPMSnewRoot	1: swSingleIPMSID 2: swSingleIPMSMacAddr	V2	SingleIP.mib
swSingleIPMSTopologyChange	1: swSingleIPMSID 2: swSingleIPMSMacAddr	V2	SingleIP.mib

Appendix D RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the DES-3200 is used in the following modules: 802.1X (Port-based and Host-based), and MAC-based Access Control.

The description that follows explains the following RADIUS Attributes Assignment types:

- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign **Ingress/Egress bandwidth by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and the 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of “0” or more, than the effective bandwidth (100Mbps on an Ethernet port or 1Gbps on a Gigabit port) of the port will be set to *no_limited*.

To assign **802.1p default priority by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default	0-7	Required

	priority of the port.		

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC-based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign **VLAN by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. To use VLAN assignment, RFC3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminatior).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC-based Access Control authentication is successful, the port will be added to VLAN 3. However, if the user does not configure the VLAN attribute and authenticates successfully, the port will be kept in its original VLAN. If the VLAN attribute configured on the RADIUS server does not exist, the port will not be assigned to the requested VLAN.

To assign **ACL by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for an ACL. The RADIUS ACL assignment is only used in MAC-based Access Control.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	12 (for ACL profile) 13 (for ACL rule)	Required
Attribute-Specific Field	Used to assign the ACL profile or rule.	ACL Command For example: ACL profile: **create access_profile profile_id 1 profile_name profile1 ethernet vlan 0xFFF**; ACL rule: **config**	Required

		access_profile profile_id 1 add access_id auto_assign ethernet vlan_id 1 port all deny;	

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: **create access_profile profile_id 1 profile_name profile1 ethernet vlan 0xFFF**; ACL rule: **config access_profile profile_id 1 add access_id auto_assign ethernet vlan_id 1 port all deny**), and the MAC-based Access Cotntrol authentication is successful, the device will assign the ACL profiles and rules according to the RADIUS server. For more information about the ACL module, please refer to Chapter 6 Access Control List (ACL) Command List.