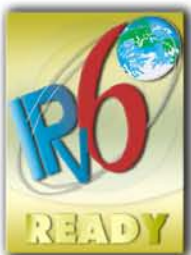




XSTACK[®]

CLI Reference Guide

Product Model: **xStack**[®] DES-3200 Series
Layer 2 Managed Fast Ethernet Switch
Release 1.28



Information in this document is subject to change without notice.

© 2011 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

March 2011 P/N 651ES3200045G

Table of Contents

INTRODUCTION	1
USING THE CONSOLE CLI	3
COMMAND SYNTAX	7
BASIC SWITCH COMMANDS	10
MODIFY BANNER AND PROMPT COMMANDS	30
SWITCH PORT COMMANDS	33
PORT SECURITY COMMANDS	37
NETWORK MANAGEMENT (SNMP) COMMANDS	43
SWITCH UTILITY COMMANDS	67
NETWORK MONITORING COMMANDS	82
MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS	99
FORWARDING DATABASE COMMANDS	115
PACKET STORM CONTROL COMMANDS	123
QOS COMMANDS	127
PORT MIRRORING COMMANDS	142
VLAN COMMANDS	145
LINK AGGREGATION COMMANDS	154
BASIC IP COMMANDS	159
IGMP SNOOPING COMMANDS	165
DHCP RELAY COMMANDS	176
802.1X COMMANDS	183
ACCESS CONTROL LIST (ACL) COMMANDS	205
TIME RANGE COMMANDS	221
SAFEGUARD ENGINE COMMANDS	223
TRAFFIC SEGMENTATION COMMANDS	225
TIME AND SNTP COMMANDS	227
ARP COMMANDS	233
ROUTING TABLE COMMANDS	237

MAC NOTIFICATION COMMANDS	243
ACCESS AUTHENTICATION CONTROL COMMANDS.....	247
SSH COMMANDS	268
SSL COMMANDS.....	275
D-LINK SINGLE IP MANAGEMENT COMMANDS.....	281
SMTP COMMANDS.....	293
CABLE DIAGNOSTICS COMMANDS	298
DHCP LOCAL RELAY COMMANDS	300
GRATUITOUS ARP COMMANDS	302
VLAN TRUNKING COMMANDS.....	306
Q-IN-Q COMMANDS.....	310
ASYMMETRIC VLAN COMMANDS	318
MLD SNOOPING COMMANDS	320
IGMP SNOOPING MULTICAST VLAN COMMANDS.....	327
LIMITED IP MULTICAST ADDRESS COMMANDS.....	333
LLDP COMMANDS	339
DOS PREVENTION COMMANDS.....	360
IP-MAC-PORT BINDING COMMANDS	366
LOOPBACK DETECTION COMMANDS.....	378
PROTOCOL VLAN COMMANDS	385
MAC-BASED VLAN COMMANDS.....	391
FLOW METER COMMANDS.....	394
MAC-BASED ACCESS CONTROL COMMANDS.....	397
ARP SPOOFING PREVENTION COMMANDS.....	413
TECHNICAL SUPPORT COMMANDS	416
COMMAND HISTORY COMMANDS	419
CONNECTIVITY FAULT MANAGEMENT COMMANDS.....	423
ETHERNET OAM COMMANDS	450
BPDU ATTACK PROTECTION COMMANDS.....	466
PER-QUEUE BANDWIDTH CONTROL COMMANDS	473

ERPS COMMANDS.....	476
NETWORK LOAD BALANCING (NLB) COMMANDS.....	486
PPPOE CIRCUIT ID INSERTION COMMANDS	492
DHCP SERVER SCREENING SETTINGS.....	496
APPENDIX A - PASSWORD RECOVERY PROCEDURE.....	500
APPENDIX B – SYSTEM LOG ENTRIES.....	502
APPENDIX C – TRAP LOG ENTRIES.....	512
APPENDIX D - RADIUS ATTRIBUTES ASSIGNMENT	516

INTRODUCTION

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

This manual provides a reference for all of the commands contained in the CLI. Configuration and management of the Switch via the Web-based management agent is discussed in the Manual. Configuration and management of the Switch via the Web-based management agent is discussed in the User's Guide.

Accessing the Switch via the Serial Port

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

- 9600 baud
- no parity
- 8 data bits
- 1 stop bit

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above are then connected to the Switch's serial port via an RS-232 DB-9 cable or RJ-45 console 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-3200-28 Fast Ethernet Switch
      Command Line Interface

      Firmware: Build 1.28.005
      Copyright(C) 2010 D-Link Corporation. All rights reserved.
UserName:
PassWord:

```

Figure 1 - 1. Initial CLI screen

There is no initial username or password. Just press the Enter key twice to display the CLI input cursor – DES-3200-28:4#. This is the command line where all commands are input.

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. Users can change the default Switch IP address to meet the specification of your networking address scheme.

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

```

Boot Procedure                                     V1.00.006
-----
Power On Self Test ..... 100%

MAC Address   : 00-63-32-28-01-01
H/W Version   : B1

Please wait, loading V1.28.005 Runtime image ..... 100%

```

Figure 1 - 2. Boot screen

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

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

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

Starting at the command line prompt, enter the command **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, users 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-3200-28:4#config ipif System ipaddress 10.73.21.11/255.0.0.0
Command: config ipif System ipaddress 10.73.21.11/8
Success.

DES-3200-28:4#
```

Figure 1 - 3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.73.21.11 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.

USING THE CONSOLE CLI

The Switch supports a console management interface that allows the user to connect to the Switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the Switch to use an SNMP-based network management application over the network.

This chapter describes how to use the console interface to access the Switch, change its settings, and monitor its operation.



Note: Switch configuration settings are saved to non-volatile RAM using the save command. The current configuration will then be retained in the Switch's NV-RAM, and reloaded when the Switch is rebooted. If the Switch is rebooted without using the save command, the last configuration saved to NV-RAM will be loaded.

Connecting to the Switch

The console interface is used by connecting the Switch to a VT100-compatible terminal or a computer running an ordinary terminal emulator program (e.g., the HyperTerminal program included with the Windows operating system) using an RS-232 DB-9 cable or RJ45 console cable. Your terminal parameters will need to be set to:

- VT-100 compatible
- 9600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

Users can also access the same functions over a Telnet interface. Once users have set an IP address for your Switch, users can use a Telnet program (in VT-100 compatible terminal mode) to access and control the Switch. All of the screens are identical, whether accessed from the console port or from a Telnet interface.

After the Switch reboots and users have logged in, the console looks like this:

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

Firmware: Build 1.28.005
Copyright(C) 2010 D-Link Corporation. All rights reserved.
UserName:
PassWord:
DES-3200-28:4#
```

Figure 2 - 1. Initial Console Screen after logging in

Commands are entered at the command prompt, DES-3200-28:4#.

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


```

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

```

Figure 2 - 2. The ? Command

When users enter a command without its required parameters, the CLI will prompt users with Next possible completions: message.

```

DES-3200-28:4#config account
Command: config account

Next possible completions:
<username>

DES-3200-28:4#

```

Figure 2 - 3. Example Command Parameter Help

In this case, the command config account was entered without the parameter <username>. The CLI will then prompt users 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-3200-28:4#config account
Command: config account

Next possible completions:
<username>

DES-3200-28:4#config account
Command: config account

Next possible completions:
<username>

DES-3200-28:4#
    
```

Figure 2 - 4. Using the Up Arrow to Re-enter a Command

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-3200-28:4#the

Available commands:
..                ?                cable_diag        clear
config            create                delete            dir
disable           download              enable            login
logout            ping                 ping6             reboot
reconfig          reset                save              show
smtp              telnet               traceroute        upload

DES-3200-28:4#
    
```

Figure 2 - 5. The Next Available Commands Prompt

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, if users enter the show command with no additional parameters, the CLI will then display all of the possible next parameters.

```

DES-3200-28:4#show
Command: show

Next possible completions:
802.1p          802.1x          access_profile  account
acct_client     address_binding arp_spoofing_prevention
auth_session_statistics  auth_statistics  authen
authen_enable  authen_login    authen_policy   authorization
autoconfig     bandwidth_control  bpdu_tunnel     command_history
config         cos              cpu_access_profile
dhcp_local_relay  dhcp_relay       dos_prevention
dot1v_protocol_group  dscp_mapping     error
fdb           firmware        flow_meter      gratuitous_arp
greeting_message  gvrp           igmp            igmp_snooping
ipif          ipif_ipv6_link_local_auto  iproute
ipv6         ipv6route       jumbo_frame     lacp_ports
limited_multicast_addr  link_aggregation  lldp
log          log_save_timing  loopdetect
mac_based_access_control  mac_based_access_control_local
mac_based_vlan  mac_notification  max_mcast_group
mcast_filter_profile  mirror           mld_snooping
multicast      multicast_fdb    packet          port
port_security  ports           pvid           qinq
radius        router_ports    safeguard_engine  scheduling
scheduling_mechanism  serial_port     session
sim          smtp           snmp           sntp
ssh         ssl            stp            switch
syslog      tech_support   terminal_line   time
time_range  traffic       traffic_segmentation
trusted_host  utilization    vlan           vlan_translation
vlan_trunk

DES-3200-28:4#

```

Figure 2 - 6. Next possible completions: Show Command

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.

COMMAND SYNTAX

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual.



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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	config ipif <System> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable]}] bootp dhcp]
Description	In the above syntax example, users must supply an IP interface name in the <System> space, a VLAN name in the <vlan_name 32> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	config ipif System ipaddress 10.24.22.5/8 vlan Design state enable

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	create account [admin user] <username 15>
Description	In the above syntax example, users must specify either an admin or a user level account to be created. Do not type the square brackets.
Example Command	create account admin ctsnow

vertical bar	
Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	create account [admin user] <username 15>
Description	In the above syntax example, users must specify either admin, or user. Do not type the vertical bar.
Example Command	create account admin ctsnow

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	reset {[config system]} {force_agree}
Description	In the first part of the above syntax example, users have the option to specify config or system. It is not necessary to specify either optional value, however the effect of the system reset is dependent on which, if any, value is specified. Therefore, with this example there are three possible outcomes of performing a system reset. Do not type the braces.
Example command	reset config

(parentheses)	
Purpose	Indicates at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified.
Syntax	config dhcp_relay {hops <value 1-16> time <sec 0-65535>}(1)
Description	In the above syntax example, 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.
Example command	config dhcp_relay hops 3

Line Editing Key Usage	
Delete	Deletes the character under the cursor and then shifts the remaining characters in the line to the left.
Backspace	Deletes the character to the left of the cursor and then shifts the remaining characters in the line to the left.
Insert or Ctrl+R	Toggle on and off. When toggled on, inserts text and shifts previous text to the right.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Up Arrow	Repeats the previously entered command. Each time the up arrow is pressed, the command previous to that displayed appears. This way it is possible to review the command history for the current session. Use the down arrow to progress sequentially forward through the command history list.
Down Arrow	The down arrow will display the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.
Tab	Shifts the cursor to the next field to the left.

Multiple Page Display Control Keys	
Space	Displays the next page.

CTRL+c	Stops the display of remaining pages when multiple pages are to be displayed.
ESC	Stops the display of remaining pages when multiple pages are to be displayed.
n	Displays the next page.
p	Displays the previous page.
q	Stops the display of remaining pages when multiple pages are to be displayed.
r	Refreshes the pages currently displayed.
a	Displays the remaining pages without pausing between pages.
Enter	Displays the next line or table entry.

BASIC SWITCH COMMANDS

The Basic Switch commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
enable password encryption	
disable password encryption	
create account	[admin user] <username 15>
config account	<username> {encrypt [plain_text sha_1] <password>}
show account	
delete account	<username>
show session	
show switch	
show serial_port	
config serial_port	{baud_rate [9600 19200 38400 115200] auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes]} (1)
enable clipaging	
disable clipaging	
enable telnet	{<tcp_port_number 1-65535>}
disable telnet	
telnet	<ipaddr> {tcp_port <value 0-65535>}
enable web	{<tcp_port_number 1-65535>}
disable web	
save	{ [config log all]}
reboot	{force_agree}
reset	{[config system]} { force_agree}
login	
logout	
show config	[current_config config_in_nvram]
config terminal_line	[default <value 20-80>]
show terminal_line	
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	

Each command is listed, in detail, in the following sections:

enable password encryption

Purpose	Used to enable password encryption on a user account.
Syntax	enable password encryption
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system at a time in the future. If the password encryption is enabled, the password will be in encrypted form. If password encryption is disabled and the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enabled password encryption command, the password will still be in encrypted form. It can not revert back to plain text.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable password encryption on the Switch.

```
DES-3200-28:4#enable password encryption
Command: enable password encryption

Success.

DES-3200-28:4#
```

disable password encryption

Purpose	Used to disable password encryption on a user account.
Syntax	disable password encryption
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system at a time in the future. If the password encryption is enabled, the password will be in encrypted form. If password encryption is disabled and the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enabled password encryption command, the password will still be in encrypted form. It can not revert back to plain text.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable password encryption on the Switch.

```
DES-3200-28:4#disable password encryption
Command: disable password encryption

Success.

DES-3200-28:4#
```


create account

Purpose	Used to create user accounts.
Syntax	create account [admin user] <username 15>
Description	This command is used to create user accounts that consist of a username of 1 to 15 characters and a password of 0 to 15 characters. Up to eight user accounts can be created.
Parameters	admin <username> – Name of the administrator account. user <username> – Name of the user account.
Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.

Example usage:

To create an administrator-level user account with the username “dlink”.

```
DES-3200-28:4#create account admin dlink
Command: create account admin dlink

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

Success.

DES-3200-28:4#
```



NOTICE: In the case of lost passwords or password corruption, please refer to Appendix C Password Recovery Procedure, at the end of this manual which will guide you through the steps necessary to resolve this issue.

config account

Purpose	Used to configure user accounts.
Syntax	config account <username> {encrypt [plain_text sha_1] <password>}
Description	<p>This command is used to configure a user account that has been created using the create account command. 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.</p> <p>If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-1.</p>
Parameters	<p><username> – The name of the account. The account must already be defined.</p> <p>plain_text – Select to specify the password in plain text form.</p> <p>sha_1 – Select to specify the password in the SHA-1 encrypted form.</p> <p>password – The password for the usefr account. The length of the 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.</p>
Restrictions	<p>Only Administrator-level users can issue this command.</p> <p>Usernames can be between 1 and 15 characters.</p> <p>Passwords can be between 0 and 15 characters.</p>

Example usage:

To configure the user password of “dlink” account:

```
DES-3200-28:4#config account dlink
Command: config account dlink

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

Success.

DES-3200-28:4#
```

show account

Purpose	Used to display user accounts.
Syntax	show account
Description	This command is used to display all user accounts created on the Switch. Up to eight user accounts can exist at one time.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the accounts that have been created:

```
DES-3200-28:4#show account
Command: show account

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

Total Entries: 1

DES-3200-28:4#
```

delete account

Purpose	Used to delete an existing user account.
Syntax	delete account <username>
Description	This command is used to delete a user account that has been created using the create account command.
Parameters	<username> – The name of the account to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account “dlink”:

```
DES-3200-28:4#delete account dlink
Command: delete account dlink

Success.

DES-3200-28:4#
```

show session

Purpose	Used to display a list of currently logged-in users.
Syntax	show session
Description	This command is used to display a list of all the users that are logged-in at the time the command is issued.
Parameters	None.
Restrictions	None.

Example usage:

To display the way that the users logged in:

```
DES-3200-28:4#show session
Command: show session

ID      Login Time          Live Time           From              Level  Name
-----
8       0/00/00 00:00:37    0:36:15:410       Serial Port       4       Anonymous

Total Entries: 1

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

show switch

Purpose	Used to display general information about the Switch.
Syntax	show switch
Description	This command is used to display information about the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch's information:

```
DES-3200-28:4#show switch
Command: show switch

Device Type       : DES-3200-28 Fast Ethernet Switch
MAC Address       : 00-63-32-28-01-01
IP Address        : 10.90.90.90 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.006
Firmware Version  : Build 1.28.005
Hardware Version  : B1
System Name       :
System Location   :
System Uptime     : 0 days, 2 hours, 53 minutes, 20 seconds
System Contact    :
Spanning Tree     : Enabled
GVRP              : Disabled
IGMP Snooping    : Disabled
VLAN Trunk        : Disabled
802.1X           : Enabled
Telnet           : Enabled (TCP 23)
Web               : Enabled (TCP 80)
RMON              : Enabled
SSH              : Disabled
SSL              : Disabled
CLI Paging        : Enabled
Syslog Global State: Disabled
Dual Image        : Supported
Password Encryption Status : Disabled

DES-3200-28:4#
```

show serial_port

Purpose	Used to display the current serial port settings.
Syntax	show serial_port
Description	This command is used to display the current serial port settings.
Parameters	None.
Restrictions	None

Example usage:

To display the serial port setting:

```
DES-3200-28:4#show serial_port
Command: show serial_port

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

DES-3200-28:4#
```

config serial_port

Purpose	Used to configure the serial port.
Syntax	config serial_port { baud_rate [9600 19200 38400 115200] auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes] } (1)
Description	This command is used to configure the serial port's baud rate and auto logout settings.
Parameters	<p>baud_rate [9600 19200 38400 115200] – The serial bit rate that will be used to communicate with the management host. There are four options: 9600, 19200, 38400, and 115200.</p> <p>never – No time limit on the length of time the console can be open with no user input.</p> <p>2_minutes – The console will log out the current user if there is no user input for 2 minutes.</p> <p>5_minutes – The console will log out the current user if there is no user input for 5 minutes.</p> <p>10_minutes – The console will log out the current user if there is no user input for 10 minutes.</p> <p>15_minutes – The console will log out the current user if there is no user input for 15 minutes.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the baud rate:

```
DES-3200-28:4#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

DES-3200-28:4#
```

enable clipaging

Purpose	Used to pause the scrolling of the console screen when a command displays more than one page.
Syntax	enable clipaging
Description	This command is used when issuing a command which causes the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page. The default setting is enabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3200-28:4#enable clipaging
Command: enable clipaging

Success.

DES-3200-28:4#
```

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when a command displays more than one screen of information.
Syntax	disable clipaging
Description	This command is used to disable the pausing of the console screen at the end of each page when a command would display more than one screen of information.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3200-28:4#disable clipaging
Command: disable clipaging

Success.

DES-3200-28:4#
```


enable telnet

Purpose	Used to enable communication with and management of the Switch using the Telnet protocol.
Syntax	enable telnet {<tcp_port_number 1-65535>}
Description	This command is used to enable the Telnet protocol on the Switch. The user can specify the TCP port number the Switch will use to listen for Telnet requests.
Parameters	<tcp_port_number 1-65535> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable Telnet and configure port number:

```
DES-3200-28:4#enable telnet 23
Command: enable telnet 23

Success.

DES-3200-28:4#
```

disable telnet

Purpose	Used to disable the Telnet protocol on the Switch.
Syntax	disable telnet
Description	This command is used to disable the Telnet protocol on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the Telnet protocol on the Switch:

```
DES-3200-28:4#disable telnet
Command: disable telnet

Success.

DES-3200-28:4#
```

telnet	
Purpose	Used to Telnet another device on the network.
Syntax	telnet <ipaddr> {tcp_port <value 0-65535>}
Description	This command is used to connect to another device's management through Telnet.
Parameters	<p><ipaddr> – Enter the IP address of the device to connect through, using Telnet.</p> <p>tcp_port <value 0-65535> – Enter the TCP port number used to connect through. The common TCP port number for telnet is 23.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To connect to a device through telnet with an IP address of 10.53.13.99:

```
DES-3200-28:4#telnet 10.53.13.99 tcp_port 23
Command: telnet 10.53.13.99 tcp_port 23
```

enable web	
Purpose	Used to enable the HTTP-based management software on the Switch.
Syntax	enable web {<tcp_port_number 1-65535>}
Description	This command is used to enable the Web-based management software on the Switch. The user can specify the TCP port number the Switch will use to listen for Telnet requests.
Parameters	<tcp_port_number 1-65535> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” port for the Web-based management software is 80.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DES-3200-28:4#enable web 80
Command: enable web 80

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

DES-3200-28:4#
```

disable web

Purpose	Used to disable the HTTP-based management software on the Switch.
Syntax	disable web
Description	This command disables the Web-based management software on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable HTTP:

```
DES-3200-28:4#disable web
Command: disable web

Success.

DES-3200-28:4#
```

save

Purpose	Used to save changes in the Switch's configuration to non-volatile RAM.
Syntax	save {[config log all]}
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the Switch's memory each time the Switch is restarted.
Parameters	<p>config – Used to save the current configuration to a file.</p> <p>log – Used to save the current log to a file. The log file cannot be deleted.</p> <p>all – Save changes to currently activated configurations and save log. If no keywords are specified, save the changes to the configuration. If there are no keywords specified, the changes will be saved to the configuration.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To save the Switch's current configuration to non-volatile RAM:

```
DES-3200-28:4#save config
Command: save config

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

DES-3200-28:4#
```

To save the Switch's current log to non-volatile RAM:

```
DES-3200-28:4#save log
Command: save log

Saving all log information to NV-RAM..... Done.
Success.

DES-3200-28:4#
```

To save the Switch's the current configuration and log to non-volatile RAM:

```
DES-3200-28:4#save all
Command: save all

Saving all configurations and log information to NV-RAM..... Done.
Success.

DES-3200-28:4#
```

reboot

Purpose	Used to restart the Switch.
Syntax	reboot {force_agree}
Description	This command is used to restart the Switch.
Parameters	force_agree – When force_agree is specified, the Switch will be forced to restart immediately without further confirmation.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To restart the Switch:

```
DES-3200-28:4#reboot
Command: reboot
Are you sure you want to proceed with the system reboot?(Y|N)
Please wait, the switch is rebooting...
```

To force the Switch to restart:

```
DES-3200-28:4#reboot force_agree
Command: reboot force_agree

Please wait, the switch is rebooting...
```

reset	
Purpose	Used to reset the Switch to the factory default settings.
Syntax	reset {[config system]} {force_agree}
Description	This command is used to restore the Switch's configuration to the default settings assigned from the factory.
Parameters	<p>config – If the keyword 'config' is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, and the switch history log. The Switch will not save or reboot.</p> <p>system – If the keyword 'system' is specified all of the factory default settings are restored on the Switch. The Switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base.</p> <p>force_agree – When force_agree is specified, the reset command will be executed immediately without further confirmation.</p> <p>If no parameter is specified, the Switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The Switch will not save or reboot.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To restore all of the Switch's parameters to their default values except the IP address, user accounts, and Switch logs:

```
DES-3200-28:4#reset
Command: reset

Are you sure you want to proceed with system reset
except IP address, log and user account?(y/n)
Success.

DES-3200-28:4#
```

To restore all of the Switch's parameters to their default values:

```
DES-3200-28:4#reset config
Command: reset config

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

Success.

DES-3200-28:4#
```

To restore all of the Switch's parameters to their default values and have the Switch save and reboot:

```
DES-3200-28:4#reset system
Command: reset system

Are you sure you want to proceed with system reset, save and reboot?(y/n)
Load Factory Default Configuration... Done.
Saving all configurations to NV-RAM.. Done.
Please wait, the switch is rebooting...
```

login

Purpose	Used to log in a user to the Switch's console.
Syntax	login
Description	This command is used to initiate the login procedure. The user will be prompted for a Username and Password.
Parameters	None.
Restrictions	None.

Example usage:

To initiate the login procedure:

```
DES-3200-28:4#login
Command: login

UserName:
```

logout

Purpose	Used to log out a user from the Switch's console.
Syntax	logout
Description	This command terminates the current user's session on the Switch's console.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current user's console session:

```
DES-3200-28:4#logout
```

show config

Purpose	Used to collect and display all system configurations in a single CLI command.
Syntax	show config [current_config config_in_nvram]
Description	This command is used to display all system configurations. The continuous displaying configuration can be aborted by the interrupt key, which may be a sequence of a keying process or a single key. The display format should be the same as the CLI configuration command.
Parameters	current_config – Display system configuration from the DRAM database, i.e. the current system setting. config_in_nvram – Display the system configuration from NV-RAM.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display all system configurations from the DRAM database:

```
DES-3200-28:4#show config config_in_nvram
Command: show config config_in_nvram

#-----
#                               DES-3200-28 Configuration
#
#                               Firmware: Build 1.28.005
#                               Copyright(C) 2010 D-Link Corporation. All rights reserved.
#-----

# BASIC

config serial_port baud_rate 9600 auto_logout 10_minutes
# ACCOUNT LIST

# ACCOUNT END

# PASSWORD ENCRYPTION
disable password encryption
config terminal_line default
enable clipaging

# STORM

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



Note: If the downloaded configuration file has been modified and saved, the “From” item will display “local save.”

config terminal_line

Purpose	Used to configure the number of rows which can be displayed on a screen.
Syntax	config terminal_line [default <value 20-80>]
Description	This command is used to configure the number of rows which can be displayed on a screen. The default value is 24.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the terminal line to display 30 rows:

```
DES-3200-28:4#config terminal_line 30
Command: config terminal_line 30

Success.

DES-3200-28:4#
```

show terminal_line

Purpose	Used to show the number of rows which can be displayed on the screen.
Syntax	show terminal_line
Description	This command is used to show the number of rows which can be displayed on the screen.
Parameters	None.
Restrictions	None.

Example usage:

To show the current number of rows that can be displayed:

```
DES-3200-28:4#show terminal_line
Command: show terminal_line

Terminal Line : 24 (Default)

DES-3200-28:4#
```


enable jumbo_frame

Purpose	Used to enable jumbo frame.
Syntax	enable jumbo_frame
Description	This command is used to configure the jumbo frame setting as enable.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable jumbo frame:

```
DES-3200-28:4#enable jumbo_frame
Command: enable jumbo_frame

Success.

DES-3200-28:4#
```

disable jumbo_frame

Purpose	Used to disable jumbo frame.
Syntax	disable jumbo_frame
Description	This command is used to configure the jumbo frame setting as disable.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable jumbo frame:

```
DES-3200-28:4#disable jumbo_frame
Command: disable jumbo_frame

Success.

DES-3200-28:4#
```

show jumbo_frame

Purpose	Used to display the current configuration of jumbo frame.
Syntax	show jumbo_frame
Description	This command is used to display the current configuration of the jumbo frame setting.
Parameters	None.
Restrictions	None.

Example usage:

To display jumbo frame:

```
DES-3200-28:4#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State      : Enabled
Maximum Jumbo Frame Size : 2048 Bytes

DES-3200-28:4#
```

MODIFY BANNER AND PROMPT COMMANDS

The Modify Banner and Prompt commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config command_prompt	[<string 32> username default]
config greeting_message	{default}
show greeting_message	

Administrator level users can modify the login banner (greeting message) and command prompt by using the commands described below:

config command prompt

Purpose	Used to configure the command prompt.
Syntax	config command_prompt [<string 32> username default]
Description	Administrator level users can use this command to change the command prompt.
Parameters	<p>string 32 – The command prompt can be changed by entering a new name of no more that 32 characters.</p> <p>username – The command prompt will be changed to the login username.</p> <p>default – The command prompt will reset to factory default command prompt. Default = the name of the Switch model, for example “DES-3200-28”.</p>
Restrictions	<p>Only Administrator-level users can issue this command. Other restrictions include:</p> <p>If the “reset” command is executed, the modified command prompt will remain modified. However, the “reset config/reset system” command will reset the command prompt to the original factory banner.</p>

Example usage

To modify the command prompt to “AtYourService”:

```
DES-3200-28:4#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:4#
```

config greeting _message

Purpose	Used to configure the login banner (greeting message).												
Syntax	config greeting _message {default}												
Description	Users can use this command to modify the login banner (greeting message).												
Parameters	<p>default – If the user enters default to the modify banner command, then the banner will be reset to the original factory banner.</p> <p>To open the Banner Editor, click Enter after typing the config greeting_message command. Type the information to be displayed on the banner by using the commands described on the Banner Editor:</p> <table border="0"> <tr> <td>Quit without save:</td> <td>Ctrl+C</td> </tr> <tr> <td>Save and quit:</td> <td>Ctrl+W</td> </tr> <tr> <td>Move cursor:</td> <td>Left/Right/Up/Down</td> </tr> <tr> <td>Delete line:</td> <td>Ctrl+D</td> </tr> <tr> <td>Erase all setting:</td> <td>Ctrl+X</td> </tr> <tr> <td>Reload original setting:</td> <td>Ctrl+L</td> </tr> </table>	Quit without save:	Ctrl+C	Save and quit:	Ctrl+W	Move cursor:	Left/Right/Up/Down	Delete line:	Ctrl+D	Erase all setting:	Ctrl+X	Reload original setting:	Ctrl+L
Quit without save:	Ctrl+C												
Save and quit:	Ctrl+W												
Move cursor:	Left/Right/Up/Down												
Delete line:	Ctrl+D												
Erase all setting:	Ctrl+X												
Reload original setting:	Ctrl+L												
Restrictions	<p>Only Administrator-level users can issue this command. Other restrictions include:</p> <p>If the “reset” command is executed, the modified banner will remain modified. However, the “reset config/reset system” command will reset the modified banner to the original factory banner.</p> <p>The capacity of the banner is 6*80. 6 Lines and 80 characters per line.</p> <p>Ctrl+W will only save the modified banner in the DRAM. Users need to type the “save config/save all” command to save it into Flash.</p> <p>Only valid in threshold level.</p>												

Example usage:

To modify the banner:

```
DES-3200-28:4#config greeting_message
Command: config greeting_message

Greeting Messages Editor
=====

                DES-3200-28 Fast Ethernet Switch
                Command Line Interface

                Firmware: Build 1.28.005

                Copyright(C) 2010 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
-----
```

show greeting_message

Purpose	Used to view the currently configured greeting message configured on the Switch.
Syntax	show greeting_message
Description	This command is used to view the currently configured greeting message on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the currently configured greeting message:

```
DES-3200-28:4#show greeting_message
Command: show greeting_message

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

Firmware: Build 1.28.005
Copyright(C) 2010 D-Link Corporation. All rights reserved.
=====

DES-3200-28:4#
```

SWITCH PORT COMMANDS

The Switch Port commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
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] state [enable disable] learning [enable disable] [description <desc 32> clear_description] mdix [auto normal cross] (1)
show ports	{<portlist>} { [description err_disabled] }

Each command is listed, in detail, in the following sections:

config ports

Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	[<portlist> all] {medium_type [fiber copper]} {speed [auto 10_half 10_full 100_half 100_full 1000_full {[master slave]}] flow_control [enable disable] state [enable disable] learning [enable disable] [description <desc 32> clear_description] mdix [auto normal cross]} (1)
Description	This command is used to configure the Switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.
Parameters	<p>all – Configure all ports on the Switch.</p> <p><portlist> – Specifies a port or range of ports to be configured.</p> <p>medium_type [fiber copper] – If configuring the Combo ports, this defines the type of medium being configured.</p> <p>speed – Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following:</p> <ul style="list-style-type: none"> auto – Enables auto-negotiation for the specified range of ports. [10 100 1000] – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 but can be set to slower speeds. [half full] – Configures the specified range of ports as either full-duplex or half-duplex. [master slave] – The master setting (1000M/Full_M) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (1000M/Full_S) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for 1000M/Full_M, the other side of the connection must be set for 1000M/Full_S. Any other configuration will result in a link down status for both ports. <p>flow_control [enable disable] – Enable or disable flow control for the specified ports.</p> <p>state [enable disable] – Enables or disables the specified range of ports.</p> <p>learning [enable disable] – Enables or disables the MAC address learning on the specified range of ports.</p> <p>description <desc 32> – Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.</p> <p>clear_description – Enter this command to clear the port description of the selected port(s).</p> <p>mdix – Specifies the MDIX setting of the port. The MDIX setting can be auto, normal or cross. If set to normal state, the port in MDIX mode, can be connected to PC NIC using a straight cable. If set to cross state, the port in mdi mode, can be connected to a port (in mdix mode) on another switch through a straight cable.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the speed of ports 25 to 28 to be 10 Mbps, full duplex, with state enabled:

```
DES-3200-28:4#config ports 25-28 speed 10_full state enable
Command: config ports 25-28 speed 10_full state enable

Warning: For combo ports, the configuration is set to medium_type copper
Success.

DES-3200-28:4#
```

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	show ports {<portlist>} {[description err_disabled]}
Description	This command is used to display the current configurations of a range of ports. No parameters will show all ports.
Parameters	<p><portlist> – Specifies a port or range of ports to be displayed.</p> <p>description – Adding this parameter to the show ports command indicates that a previously entered port description will be included in the display.</p> <p>err_disabled – Use this to list disabled ports including connection status and reason for being disabled.</p>
Restrictions	None.

Example usage:

To display the configuration of all ports on a standalone switch:

```
DES-3200-28:4#show ports
Command show ports

Port      State/      Settings      Connection      Address
      MDI      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
-----
1         Enabled    100M/Full/Disabled  LinkDown          Enabled
2         Enabled    100M/Full/Disabled  LinkDown          Enabled
3         Enabled    100M/Full/Disabled  LinkDown          Enabled
4         Enabled    100M/Full/Disabled  LinkDown          Enabled
5         Enabled    100M/Full/Disabled  LinkDown          Enabled
6         Enabled    100M/Full/Disabled  LinkDown          Enabled
7         Enabled    100M/Full/Disabled  LinkDown          Enabled
8         Enabled    100M/Full/Disabled  LinkDown          Enabled
9         Enabled    100M/Full/Disabled  LinkDown          Enabled

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


Example usage:

To display the configuration of all ports on a standalone switch, with description:

```
DES-3200-28:4#show ports description
Command: show ports description

Port   State/      Settings          Connection        Address
      MDI       Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
-----
1      Enabled    100M/Full/Disabled  LinkDown           Enabled

Desc:
2      Enabled    100M/Full/Disabled  LinkDown           Enabled

Desc:
3      Enabled    100M/Full/Disabled  LinkDown           Enabled

Desc:
4      Enabled    100M/Full/Disabled  LinkDown           Enabled

Desc:
5      Enabled    100M/Full/Disabled  LinkDown           Enabled

Desc:
6      Enabled    100M/Full/Disabled  LinkDown           Enabled

Desc:

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

PORT SECURITY COMMANDS

The Port Security commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config port_security ports	[<auth_portlist> all] {admin_state [enable disable] max_learning_addr <max_lock_no 0-64> lock_address_mode [DeleteOnTimeout DeleteOnReset Permanent]} (1)
delete port_security_entry	vlan_name <vlan_name 32> mac_address <macaddr> port <auth_port>
clear port_security_entry	port <auth_portlist>
show port_security	{ports <auth_portlist>}
enable port_security trap_log	
disable port_security trap_log	

Each command is listed, in detail, in the following sections:

config port_security ports

Purpose	Used to configure port security settings.
Syntax	config port_security ports [<auth_portlist> all] {admin_state [enable disable] max_learning_addr <max_lock_no 0-64> lock_address_mode [DeleteOnTimeout DeleteOnReset Permanent]} (1)
Description	This command is used to configure the port security feature. Only the ports listed in the <auth_portlist> are affected.
Parameters	<p><auth_portlist> – Specifies a port or range of ports to be configured.</p> <p>all – Configure port security for all ports on the Switch.</p> <p>admin_state [enable disable] – Enable or disable port security for the listed ports.</p> <p>max_learning_addr <max_lock_no 0-64> – Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p>lock_address_mode [DeleteOnTimout DeleteOnReset Permanent] – Indicates the method of locking addresses. The user has three choices:</p> <p>DeleteOnTimeout – The locked addresses will age out after the aging timer expires (Aging Time is set using the FDB command).</p> <p>DeleteOnReset – The locked addresses will not age out until the Switch has been reset.</p> <p>Permanent – The locked addresses will not age out.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the port security:

```
DES-3200-28:4#config port_security ports 1-5 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnReset
Command: config port_security ports 1-5 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnReset

Success.

DES-3200-28:4#
```

delete port_security_entry

Purpose	Used to delete a port security entry by MAC address, port number and VLAN ID.
Syntax	delete port_security_entry vlan_name <vlan_name 32> mac_address <macaddr> port <auth_port>
Description	This command is used to delete a single, previously learned port security entry by port, VLAN name, and MAC address.
Parameters	vlan_name <vlan_name 32> – Enter the corresponding VLAN name of the port to delete. mac_address <macaddr> – Enter the corresponding MAC address, previously learned by the port, to delete. port <auth_port> – Enter the port number which has learned the previously entered MAC address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a port security entry:

```
DES-3200-28:4#delete port_security_entry vlan_name default mac_address  
00-01-30-10-2C-C7 port 6  
Command: delete port_security_entry vlan_name default mac_address 00-01-  
30-10-2C-C7 port 6  
  
Success.  
  
DES-3200-28:4#
```

clear port_security_entry

Purpose	Used to clear MAC address entries learned from a specified port for the port security function.
Syntax	clear port_security_entry ports <auth_portlist>
Description	This command is used to clear MAC address entries which were learned by the Switch by a specified port. This command only relates to the port security function.
Parameters	<auth_portlist> – Specifies a port or port range to clear.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear a port security entry by port:

```
DES-3200-28:4# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DES-3200-28:4#
```

show port_security

Purpose	Used to display the current port security configuration.
Syntax	show port_security {ports <auth_portlist>}
Description	This command is used to display port security information of the Switch's ports. The information displayed includes port security, admin state, maximum number of learning address and lock mode.
Parameters	<auth_portlist> – Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DES-3200-28:4#show port_security ports 1-10
Command: show port_security ports 1-10

Port_security Trap/Log : Disabled

Port      Admin State      Max. Learning Addr.  Lock Address Mode
----      -
1         Disabled         1                    DeleteOnTimeout
2         Disabled         1                    DeleteOnTimeout
3         Disabled         1                    DeleteOnTimeout
4         Disabled         1                    DeleteOnTimeout
5         Disabled         1                    DeleteOnTimeout
6         Disabled         1                    DeleteOnTimeout
7         Disabled         1                    DeleteOnTimeout
8         Disabled         1                    DeleteOnTimeout
9         Disabled         1                    DeleteOnTimeout
10        Disabled         1                    DeleteOnTimeout

DES-3200-28:4#
```

enable port_security trap_log

Purpose	Used to enable the trap log for port security.
Syntax	enable port_security trap_log
Description	This command, along with the disable port_security trap_log, will enable the sending of log messages to the Switch's log and SNMP agent when the port security of the Switch has been triggered.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the port security trap log setting:

```
DES-3200-28:4#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3200-28:4#
```

disable port_security trap_log

Purpose	Used to disable the trap log for port security.
Syntax	disable port_security trap_log
Description	This command, along with the enable port_security trap_log, will disable the sending of log messages to the Switch's log and SNMP agent when the port security of the Switch has been triggered.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the port security trap log setting:

```
DES-3200-28:4#disable port_security trap_log
Command: disable port_security trap_log

Success.

DES-3200-28:4#
```

NETWORK MANAGEMENT (SNMP) COMMANDS

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. Users can specify which version of the SNMP users want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

SNMP Version	Authentication Method	Description
v1	Community String	Community String is used for authentication – NoAuthNoPriv
v2c	Community String	Community String is used for authentication – NoAuthNoPriv
v3	Username	Username is used for authentication – NoAuthNoPriv
v3	MD5 or SHA	Authentication is based on the HMAC-MD5 or HMAC-SHA algorithms – AuthNoPriv
v3	MD5 DES or SHA DES	Authentication is based on the HMAC-MD5 or HMAC-SHA algorithms – AuthPriv. DES 56-bit encryption is added based on the CBC-DES (DES-56) standard

The Network Management commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
create snmp user	<SNMP_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	<SNMP_name 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included excluded]
delete snmp view	<view_name 32> [all oid]
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> view <view_name 32> [read_only read_write]
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID 10-64>
show snmp engineID	
create snmp group	<groupname 32> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] {read_view <view_name 32> write_view <view_name 32> notify_view <view_name 32>} (1)
delete snmp group	<groupname 32>
show snmp groups	
create snmp	[host <ipaddr> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] <auth_string 32>
delete snmp	[host <ipaddr>]

Command	Parameters
show snmp host	{<ipaddr>}
create trusted_host	[<ipaddr> network<network_address>]
delete trusted_host	[ipaddr<ipaddr> network<network_address> all]
show trusted_host	
enable snmp	[authenticate_traps linkchange_traps traps]
disable snmp	[authenticate_traps linkchange_traps traps]
disable snmp linkchange_traps	
enable snmp linkchange_traps	
config snmp linkchange_traps ports	[all <portlist>] [enable disable]
show snmp traps	{linkchange_traps { ports <portlist> } }
config snmp system_contact	{<sw_contact>}
config snmp system_location	{<sw_location>}
config snmp system_name	{<sw_name>}
enable rmon	
disable rmon	

Each command is listed, in detail, in the following sections:

create snmp user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	create snmp user <SNMP_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> sha <auth_password 8-20>] priv [none des <priv_password 8-16>] by_key auth [md5 <auth_key 32-32> sha <auth_key 40-40>] priv [none des <priv_key 32-32>]]}
Description	<p>This command is used to create a new SNMP user and adds the user to an SNMP group that is also created by this command. SNMP ensures:</p> <p>Message integrity – Ensures that packets have not been tampered with during transit.</p> <p>Authentication – Determines if an SNMP message is from a valid source.</p> <p>Encryption – Scrambles the contents of messages to prevent it from being viewed by an unauthorized source.</p>
Parameters	<p><SNMP_name 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.</p> <p><groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p>encrypted – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose:</p> <ul style="list-style-type: none"> by_password – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the auth_password below. This method is recommended. by_key – Requires the SNMP user to enter an encryption key for authentication and privacy. The key is defined by specifying the key in hex form. This method is not recommended. <p>auth – The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are:</p> <ul style="list-style-type: none"> md5 – Specifies that the HMAC-MD5-96 authentication level will be used. md5 may be utilized by entering one of the following: <ul style="list-style-type: none"> <auth password 8-16> – An alphanumeric string of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host. <auth_key 32-32> – Enter an alphanumeric string of exactly 32 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host. sha – Specifies that the HMAC-SHA-96 authentication level will be used. <auth password 8-20> – An alphanumeric string of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host. <auth_key 40-40> – Enter an alphanumeric string of exactly 40 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host. <p>priv – Adding the priv (privacy) parameter will allow for encryption in addition to the authentication algorithm for higher security. The user may choose:</p> <ul style="list-style-type: none"> des – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using: <ul style="list-style-type: none"> <priv_password 8-16> – An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent. <priv_key 32-32> – Enter an alphanumeric key string of exactly 32 characters, in hex form, that will be used to encrypt the contents of messages the host sends to the agent. none – Adding this parameter will add no encryption.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DES-3200-28:4#create snmp user dlink default encrypted by_password auth md5
knickerbockers priv none
Command: create snmp user dlink default encrypted by_password auth md5
knickerbockers priv none

Success.

DES-3200-28:4#
```

delete snmp user

Purpose	Used to remove an SNMP user from an SNMP group and also to delete the associated SNMP group.
Syntax	delete snmp user <SNMP_name 32>
Description	This command is used to remove an SNMP user from its SNMP group and then delete the associated SNMP group.
Parameters	<SNMP_name 32> – An alphanumeric string of up to 32 characters that identifies the SNMP user that will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a previously entered SNMP user on the Switch:

```
DES-3200-28:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-3200-28:4#
```

show snmp user

Purpose	Used to display information about each SNMP username in the SNMP group username table.
Syntax	show snmp user
Description	This command is used to display information about each SNMP username in the SNMP group username table.
Parameters	None.
Restrictions	None.

Example usage:

To display the SNMP users currently configured on the Switch:

```
DES-3200-28:4#show snmp user
Command: show snmp user

Username          Group Name        SNMP Version Auth-Protocol PrivProtocol
-----
initial          initial          V3              None          None

Total Entries: 1

DES-3200-28:4#
```

create snmp view	
Purpose	Used to assign views to community strings to limit which MIB objects and SNMP manager can access.
Syntax	create snmp view <view_name 32> <oid> view_type [included excluded]
Description	This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	<p><view_name 32> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created.</p> <p><oid> – The object ID that identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.</p> <p>view type – Sets the view type to be:</p> <p>included – Include this object in the list of objects that an SNMP manager can access.</p> <p>excluded – Exclude this object from the list of objects that an SNMP manager can access.</p>
Restrictions	None.

Example usage:

To create an SNMP view:

```
DES-3200-28:4#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-3200-28:4#
```

delete snmp view

Purpose	Used to remove an SNMP view entry previously created on the Switch.
Syntax	delete snmp view <view_name 32> [all <oid>]
Description	This command is used to remove an SNMP view previously created on the Switch.
Parameters	<p><view_name 32> – An alphanumeric string of up to 32 characters that identifies the SNMP view to be deleted.</p> <p>all – Specifies that all of the SNMP views on the Switch will be deleted.</p> <p><oid> – The object ID that identifies an object tree (MIB tree) that will be deleted from the Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DES-3200-28:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-3200-28:4#
```

show snmp view

Purpose	Used to display an SNMP view previously created on the Switch.
Syntax	show snmp view {<view_name 32>}
Description	This command is used to display an SNMP view previously created on the Switch.
Parameters	<view_name 32> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be displayed.
Restrictions	None.

Example usage:

To display SNMP view configuration:

```
DES-3200-28:4#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name          Subtree          View Type
-----
restricted         1.3.6.1.2.1.1   Included
restricted         1.3.6.1.2.1.11  Included
restricted         1.3.6.1.6.3.10.2.1 Included
restricted         1.3.6.1.6.3.11.2.1 Included
restricted         1.3.6.1.6.3.15.1.1 Included
CommunityView      1                Included
CommunityView      1.3.6.1.6.3      Excluded
CommunityView      1.3.6.1.6.3.1   Included
Total Entries   : 8

DES-3200-28:4#
```

create snmp community

Purpose	Used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string: An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community. read_write or read_only level permission for the MIB objects accessible to the SNMP community.
Syntax	create snmp community <community_string 32> view <view_name 32> [read_only read_write]
Description	This command is used to create an SNMP community string and to assign access-limiting characteristics to this community string.
Parameters	<community_string 32> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch’s SNMP agent. view <view_name 32> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. read_only – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch. read_write – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the Switch.
Restrictions	None.

Example usage:

To create the SNMP community string “dlink”:

```
DES-3200-28:4#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DES-3200-28:4#
```

delete snmp community

Purpose	Used to remove a specific SNMP community string from the Switch.
Syntax	delete snmp community <community_string 32>
Description	This command is used to remove a previously defined SNMP community string from the Switch.
Parameters	<community_string 32> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch’s SNMP agent.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the SNMP community string “dlink”:

```
DES-3200-28:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-3200-28:4#
```

show snmp community

Purpose	Used to display SNMP community strings configured on the Switch.
Syntax	show snmp community {<community_string 32>}
Description	This command is used to display SNMP community strings that are configured on the Switch.
Parameters	<community_string 32> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch’s SNMP agent.
Restrictions	None.

Example usage:

To display the currently entered SNMP community strings:

```
DES-3200-28:4#show snmp community
Command: show snmp community

SNMP Community Table

Community Name      View Name          Access Right
-----
private            CommunityView     read_write
public             CommunityView     read_only
dlink              ReadView          read_write

Total Entries: 3

DES-3200-28:4#
```

config snmp engineID	
Purpose	Used to configure an identifier for the SNMP engine on the Switch.
Syntax	config snmp engineID <snmp_engineID 10-64>
Description	This command is used to configure an identifier for the SNMP engine on the Switch.
Parameters	<snmp_engineID 10-64> – An alphanumeric string that will be used to identify the SNMP engine on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To give the SNMP agent on the Switch the name “0035636666”:

```
DES-3200-28:4#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DES-3200-28:4#
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the Switch.
Syntax	show snmp engineID
Description	This command is used to display the identification of the SNMP engine on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the current name of the SNMP engine on the Switch:

```
DES-3200-28:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DES-3200-28:4#
```

create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	create snmp group <groupname 32> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] {read_view <view_name 32> write_view <view_name 32> notify_view <view_name 32>} (1)
Description	This command is used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	<p><groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p>v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p>v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p>v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <p>Message integrity – Ensures that packets have not been tampered with during transit.</p> <p>Authentication – Determines if an SNMP message is from a valid source.</p> <p>Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source.</p> <p>noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>auth_priv – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manager will be encrypted.</p> <p>read_view – Specifies that the SNMP group being created can request SNMP messages.</p> <p>write_view – Specifies that the SNMP group being created has write privileges.</p> <p>notify_view – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent.</p> <p><view_name 32> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.</p>
Restrictions	None.

Example usage:

To create an SNMP group named “sg1:”

```
DES-3200-28:4#create snmp group sg1 v3 noauth_nopriv read_view v1 write_view
v1 notify_view v1
Command: create snmp group sg1 v3 noauth_nopriv read_view v1 write_view v1
notify_view v1

Success.

DES-3200-28:4#
```

delete snmp group

Purpose	Used to remove an SNMP group from the Switch.
Syntax	delete snmp group <groupname 32>
Description	This command is used to remove an SNMP group from the Switch.
Parameters	<groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the SNMP group named “sg1”.

```
DES-3200-28:4#delete snmp group sg1
Command: delete snmp group sg1

Success.

DES-3200-28:4#
```

show snmp groups

Purpose	Used to display the group names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Syntax	show snmp groups
Description	This command is used to display the group names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Parameters	None.
Restrictions	None.

Example usage:

To display the currently configured SNMP groups on the Switch:

```
DES-3200-28:4#show snmp groups
Command: show snmp groups
Vacm Access Table Settings

Group Name       : Group3
ReadView Name    : ReadView
WriteView Name   : WriteView
Notify View Name : NotifyView
Security Model   : SNMPv3
Security Level   : NoAuthNoPriv

Group Name       : Group4
ReadView Name    : ReadView
WriteView Name   : WriteView
Notify View Name : NotifyView
Security Model   : SNMPv3
Security Level   : authNoPriv

Group Name       : Group5
ReadView Name    : ReadView
WriteView Name   : WriteView
Notify View Name : NotifyView
Security Model   : SNMPv3
Security Level   : authNoPriv

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

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

Total Entries: 5

DES-3200-28:4#
```

create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	create snmp [host <ipaddr>] [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv] <auth_string 32>
Description	This command is used to create a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<p><ipaddr> – The IP address of the remote management station that will serve as the SNMP host for the Switch.</p> <p>v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p>v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p>v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <p>Message integrity – ensures that packets have not been tampered with during transit.</p> <p>Authentication – determines if an SNMP message is from a valid source.</p> <p>Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source.</p> <p>noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>auth_priv – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.</p> <p><auth_string 32> – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.</p>
Restrictions	None.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-3200-28:4#create snmp host 10.48.74.100 v3 auth_priv public
Command: create snmp host 10.48.74.100 v3 auth_priv public

Success.

DES-3200-28:4#
```

delete snmp host

Purpose	Used to remove a recipient of SNMP traps generated by the Switch's
----------------	--

delete snmp host

	SNMP agent.
Syntax	delete snmp [host <ipaddr>]
Description	This command is used to delete a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<ipaddr> – The IP address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an SNMP host entry:

```
DES-3200-28:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DES-3200-28:4#
```

show snmp host

Purpose	Used to display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	show snmp host {<ipaddr>}
Description	This command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps that are generated by the Switch's SNMP agent.
Parameters	<ipaddr> – The IP address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DES-3200-28:4#show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version  Community Name / SNMPv3 User Name
-----
10.48.76.23     V3 noauthnopriv  initial
10.48.74.100   V2c              public

Total Entries   : 2

DES-3200-28:4#
```

create trusted_host

Purpose	Used to create a trusted host.
Syntax	create trusted_host [<ipaddr> network <network_address>]

create trusted_host

Description	This command is used to create a trusted host. The Switch allows users to specify up to ten IP addresses that are allowed to manage the Switch via in-band SNMP or Telnet-based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.
Parameters	<ipaddr> – The IP address of the trusted host to be created. <network_address> – The IP address and netmask of the trusted host to be created.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a trusted host:

```
DES-3200-28:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DES-3200-28:4#
```

To create a trusted host network:

```
DES-3200-28:4#create trusted_host network 10.48.0.0/16
Command: create trusted_host network 10.48.0.0/16

Success.

DES-3200-28:4#
```

delete trusted_host

Purpose	Used to delete a trusted host entry made using the create trusted_host command above.
Syntax	delete trusted_host [ipaddr <ipaddr> network <network_address> all]
Description	This command is used to delete a trusted host entry made using the create trusted_host command above.
Parameters	<ipaddr> – The IP address of the trusted host. <network_address> – The network address of the trusted network. all – All trusted hosts will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DES-3200-28:4#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

DES-3200-28:4#
```

To delete a trusted host network with a network address 10.62.0.0/16:

```
DES-3200-28:4#delete trusted_host network 10.62.0.0/16
Command: delete trusted_host network 10.62.0.0/16

Success.

DES-3200-28:4#
```

To delete all trusted host entries:

```
DES-3200-28:4#delete trusted_host all
Command: delete trusted_host all

Success.

DES-3200-28:4#
```

show trusted_host	
Purpose	Used to display a list of trusted hosts entered on the Switch using the create trusted_host command above.
Syntax	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.
Parameters	None.
Restrictions	None.

Example Usage:

To display the list of trust hosts:

```
DES-3200-28:4#show trusted_host
Command: show trusted_host

Management Stations

IP Address/Netmask
-----
10.53.13.94/32

Total Entries: 1

DES-3200-28:4#
```

enable snmp	
Purpose	Used to enable SNMP trap support.
Syntax	enable snmp [authenticate_traps linkchange_traps traps]
Description	This command is used to enable SNMP trap support on the Switch.
Parameters	authenticate_traps – This is to enable SNMP authentication trap support. linkchange_traps – This is to enable SNMP linkchange trap support. traps – This is to enable SNMP trap support.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SNMP trap support on the Switch:

```
DES-3200-28:4#enable snmp traps
Command: enable snmp traps

Success.

DES-3200-28:4#
```

To enable SNMP linkchange trap support on the Switch:

```
DES-3200-28:4#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DES-3200-28:4#
```

To enable SNMP authentication trap support:

```
DES-3200-28:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DES-3200-28:4#
```

disable snmp

Purpose	Used to disable SNMP trap support on the Switch.
Syntax	disable snmp [authenticate_traps linkchange_traps traps]
Description	This command is used to disable SNMP trap support on the Switch.
Parameters	authenticate_traps – This is to disable SNMP authentication trap support. linkchange_traps – This is to disable SNMP linkchange trap support. traps – This is to disable SNMP trap support.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SNMP authentication trap support:

```
DES-3200-28:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DES-3200-28:4#
```

To disable SNMP linkchange trap support:

```
DES-3200-28:4#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DES-3200-28:4#
```

To prevent SNMP traps from being sent from the Switch:

```
DES-3200-28:4#disable snmp traps
Command: disable snmp traps

Success.

DES-3200-28:4#
```

config snmp linkchange_traps ports	
Purpose	Used to configure the sending of linkchange traps and per port control for sending of change traps.
Syntax	config snmp linkchange_traps ports [all <portlist>] [enable disable]
Description	This command is used to configure the sending of linkchange traps and per port control for the sending of change traps.
Parameters	all – To specify all ports. <portlist> - To specify a port range. enable – To enable the sending of a link change trap for this port. disable - To disable the sending of a link change trap for this port.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure SNMP linkchange traps for ports 1 to 4:

```
DES-3200-28:4#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DES-3200-28:4#
```

show snmp traps	
Purpose	Used to show SNMP trap support on the Switch.
Syntax	show snmp traps {linkchange_traps { ports <portlist> } }
Description	This command is used to view the SNMP trap support status currently configured on the Switch.
Parameters	linkchange_traps – This displays the current SNMP linkchange trap status. <portlist> – This specifies a list of ports to display SNMP trap support.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DES-3200-28:4#show snmp traps
Command: show snmp traps

SNMP Traps           : Enabled
Authenticate Traps  : Enabled
Linkchange Traps     : Enabled

DES-3200-28:4#
```

config snmp system_contact

Purpose	Used to enter the name of a contact person who is responsible for the Switch.
Syntax	config snmp system_contact {<sw_contact>}
Description	This command is used to enter the name and/or other information to identify a contact person who is responsible for the Switch. A maximum of 128 characters can be used.
Parameters	<sw_contact> – A maximum of 128 characters is allowed. A NULL string is accepted if there is no contact.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the Switch contact to “MIS Department II”:

```
DES-3200-28:4#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DES-3200-28:4#
```

config snmp system_location

Purpose	Used to enter a description of the location of the Switch.
Syntax	config snmp system_location {<sw_location>}
Description	This command is used to enter a description of the location of the Switch. A maximum of 128 characters can be used.
Parameters	<sw_location> – A maximum of 128 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3200-28:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3200-28:4#
```

config snmp system_name	
Purpose	Used to configure the name for the Switch.
Syntax	config snmp system_name {<sw_name>}
Description	This command is used to configure the name of the Switch.
Parameters	<sw_name> – A maximum of 128 characters is allowed. A NULL string is accepted if no name is desired.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the Switch name for “DES-3200-28 Switch”:

```
DES-3200-28:4#config snmp system_name DES-3200-28 Switch
Command: config snmp system_name DES-3200-28 Switch

Success.

DES-3200-28:4#
```

enable rmon	
Purpose	Used to enable RMON on the Switch.
Syntax	enable rmon
Description	This command is used, in conjunction with the disable rmon command below, to enable and disable remote monitoring (RMON) on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To enable RMON:

```
DES-3200-28:4#enable rmon
Command: enable rmon

Success.

DES-3200-28:4#
```

disable rmon

Purpose	Used to disable RMON on the Switch.
Syntax	disable rmon
Description	This command is used, in conjunction with the enable rmon command above, to enable and disable remote monitoring (RMON) on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To disable RMON:

```
DES-3200-28:4#disable rmon
Command: disable rmon

Success.

DES-3200-28:4#
```

SWITCH UTILITY COMMANDS

The Switch Utility commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
download	[firmware_fromTFTP [<ipaddr> <ipv6addr>] <path_filename 64> image_id <value 1-2> cfg_fromTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {increment}]
config firmware	image_id <value 1-2> [delete boot_up]
show firmware information	
show config	[current_config config_in_nvram]
upload	[cfg_toTFTP log_toTFTP] [<ipaddr> <ipv6addr>] <path_filename 64>
enable autoconfig	
disable autoconfig	
show autoconfig	
ping	<ipaddr> {times <value 0-255>} {size <value 1-60000>} {timeout <sec 1-99>}
ping6	<ipv6addr> {times <value 1-255> size <value 1-6000>} timeout <value 1-10>}
traceroute	<ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}
config terminal _line	[default <value 20-80>]
show terminal_line	

Each command is listed, in detail, in the following sections:

download	
Purpose	Used to download and install new firmware or a Switch configuration file from a TFTP server.
Syntax	download [firmware_fromTFTP [<ipaddr> <ipv6addr>] <path_filename 64> image_id <value 1-2> cfg_fromTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {increment}]
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	<p>firmware_fromTFTP – Download and install new firmware on the Switch from a TFTP server.</p> <p>cfg_fromTFTP – Download a switch configuration file from a TFTP server.</p> <p><ipaddr> – The IP address of the TFTP server.</p> <p><ipv6addr> – The IPv6 address of the TFTP server.</p> <p><path_filename> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3200.had.</p> <p>image_id <value 1-2> – Specify the working section ID. The Switch can hold two firmware versions for the user to select from, which are specified by section ID.</p> <p>increment – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.</p>
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only Administrator-level users can issue this command.

Example usage:

To download a configuration file:

```
DES-3200-28:4#download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt
Command: download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt

Connecting to server..... Done.
Download configuration..... Done.
Success.
DES-3200-28:4#
DES-3200-28:4##-----
DES-3200-28:4##                               DES-3200-28 Configuration
DES-3200-28:4##
DES-3200-28:4##                               Firmware: Build 1.28.005
DES-3200-28:4## Copyright(C) 2010 D-Link Corporation. All rights reserved.
DES-3200-28:4##-----
DES-3200-28:4#
DES-3200-28:4#
DES-3200-28:4## BASIC
DES-3200-28:4#
DES-3200-28:4#config serial_port baud_rate 9600 auto_logout 10_minutes
Command: config serial_port baud_rate 9600 auto_logout 10_minutes
```

The download configuration command will initiate the loading of the various settings in the order listed in the configuration file. When the file has been successfully loaded the message “End of configuration file for DES-3200-28” appears followed by the command prompt.

```
DES-3200-28:4#disable authen_policy
```

```
Command: disable authen_policy
```

```
Success.
```

```
DES-3200-28:4#
```

config firmware	
Purpose	Used to configure the firmware section image as a boot up section, or to delete the firmware section
Syntax	config firmware image_id <value 1-2> [delete boot_up]
Description	This command is used to configure the firmware section image. The user may choose to remove the firmware section or use it as a boot up section.
Parameters	image_id – Specifies the working section image. The Switch can hold two firmware versions for the user to select from, which are specified by image ID. delete – Entering this parameter will delete the specified firmware section image. boot_up – Entering this parameter will specify the firmware image ID as a boot up section image.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure firmware section image 1 as a boot up section:

```
DES-3200-28:4# config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DES-3200-28:4#
```

show firmware information

Purpose	Used to display the firmware section information.
Syntax	show firmware information
Description	This command is used to display the firmware section information.
Parameters	None.
Restrictions	None

Example usage:

To display the current firmware information on the Switch:

```
DES-3200-28:4#show firmware information
Command: show firmware information

Image ID   : 1(Boot up firmware)
Version    : 1.28.005
Size       : 3980264 Bytes
Update Time: 0000/00/00 00:09:09
From       : 10.90.90.1
User       : Anonymous(Web)

Image ID   : 2
Version    : 1.28.001
Size       : 3798872 Bytes
Update Time: 0000/00/00 01:32:32
From       : 10.63.54.1
User       : Anonymous(CONSOLE)

DES-3200-28:4#
```

show config

Purpose	Used to display the current or saved version of the configuration settings of the switch.																																				
Syntax	show config [current_config config_in_nvram]																																				
Description	<p>This command is used to display all the configuration settings that are saved to NVRAM or display the configuration settings as they are currently configured. Use the keyboard to list settings one line at a time (Enter), one page at a time (Space) or view all (a).</p> <p>The configuration settings are listed by category in the following order:</p> <table border="0"> <tr> <td>Basic (serial port, Telnet and web management status)</td> <td>ACL</td> </tr> <tr> <td>storm control</td> <td>SNTP</td> </tr> <tr> <td>IP group management</td> <td>IP route</td> </tr> <tr> <td>Syslog</td> <td>LACP</td> </tr> <tr> <td>QoS</td> <td>ARP</td> </tr> <tr> <td>port mirroring</td> <td>IP</td> </tr> <tr> <td>traffic segmentation</td> <td>IGMP snooping</td> </tr> <tr> <td>port</td> <td>access authentication control (TACACS etc.)</td> </tr> <tr> <td>port lock</td> <td>PoE</td> </tr> <tr> <td>8021x</td> <td>Bandwidth</td> </tr> <tr> <td>SNMPv3</td> <td>Time_range</td> </tr> <tr> <td>management (SNMP traps RMON)</td> <td>GM</td> </tr> <tr> <td>VLAN</td> <td>safeguard_engine</td> </tr> <tr> <td>FDB (forwarding data base)</td> <td>Banner_promp</td> </tr> <tr> <td>MAC address table notification</td> <td>SMTP</td> </tr> <tr> <td>STP</td> <td>AAA</td> </tr> <tr> <td>SSH</td> <td>DHCP_Relay</td> </tr> <tr> <td>SSL</td> <td></td> </tr> </table>	Basic (serial port, Telnet and web management status)	ACL	storm control	SNTP	IP group management	IP route	Syslog	LACP	QoS	ARP	port mirroring	IP	traffic segmentation	IGMP snooping	port	access authentication control (TACACS etc.)	port lock	PoE	8021x	Bandwidth	SNMPv3	Time_range	management (SNMP traps RMON)	GM	VLAN	safeguard_engine	FDB (forwarding data base)	Banner_promp	MAC address table notification	SMTP	STP	AAA	SSH	DHCP_Relay	SSL	
Basic (serial port, Telnet and web management status)	ACL																																				
storm control	SNTP																																				
IP group management	IP route																																				
Syslog	LACP																																				
QoS	ARP																																				
port mirroring	IP																																				
traffic segmentation	IGMP snooping																																				
port	access authentication control (TACACS etc.)																																				
port lock	PoE																																				
8021x	Bandwidth																																				
SNMPv3	Time_range																																				
management (SNMP traps RMON)	GM																																				
VLAN	safeguard_engine																																				
FDB (forwarding data base)	Banner_promp																																				
MAC address table notification	SMTP																																				
STP	AAA																																				
SSH	DHCP_Relay																																				
SSL																																					
Parameters	<p>current_config – Entering this parameter will display configurations entered without being saved to NVRAM.</p> <p>config_in_NVRAM – Entering this parameter will display configurations entered and saved to NVRAM.</p>																																				
Restrictions	Only Administrator-level users can issue this command.																																				

Example usage:

To view the current configuration settings:

```
DES-3200-28:4#show config current_config
Command: show config current_config

#-----
#
#           DES-3200-28 Configuration
#
#           Firmware: Build 1.28.005
#           Copyright(C) 2010 D-Link Corporation. All rights reserved.
#-----

# BASIC

config serial_port baud_rate 9600 auto_logout 10_minutes
# ACCOUNT LIST

# ACCOUNT END

# PASSWORD ENCRYPTION
disable password encryption
config terminal_line default
enable clipping

# STORM

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

upload	
Purpose	Used to upload the current switch settings or the switch history log to a TFTP.
Syntax	upload [cfg_toTFTP log_toTFTP] [<ipaddr> <ipv6addr>] <path_filename 64>
Description	This command is used to upload either the Switch's current settings or the Switch's history log to a TFTP server.
Parameters	<p>cfg_toTFTP – Specifies that the Switch's current settings will be uploaded to the TFTP server.</p> <p>log_toTFTP – Specifies that the switch history log will be uploaded to the TFTP server.</p> <p><ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch.</p> <p><ipv6addr> – The IPv6 address of the TFTP server.</p> <p><path_filename 64> – Specifies the location of the Switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the Switch.</p>
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only Administrator-level users can issue this command.

Example usage:

To upload a configuration file:

```
DES-3200-28:4#upload cfg_toTFTP 10.48.74.121 c:\cfg\log.txt
Command: upload cfg_toTFTP 10.48.74.121 c:\cfg\log.txt
Success.
Connecting to server..... Done.
Upload configuration.....Done.

DES-3200-28:4#
```

enable autoconfig

Purpose	Used to activate the auto configuration function for the Switch. This will load a previously saved configuration file for current use.
Syntax	enable autoconfig
Description	When autoconfig is enabled on the Switch, the DHCP reply will contain a configuration file and path name. It will then request the file from the TFTP server specified in the reply. When autoconfig is enabled, the ipif settings will automatically become DHCP client.
Parameters	None.
Restrictions	When autoconfig is enabled, the Switch becomes a DHCP client automatically (same as: config ipif System dhcp). The DHCP server must have the TFTP server IP address and configuration file name, and be configured to deliver this information in the data field of the DHCP reply packet. The TFTP server must be running and have the requested configuration file in its base directory when the request is received from the Switch. Consult the DHCP server and TFTP server software instructions for information on loading a configuration file. If the Switch is unable to complete the auto configuration process the previously saved local configuration file present in Switch memory will be loaded.



Note: Dual-purpose (DHCP/TFTP) server utility software may require entry of the configuration file name and path within the user interface. Alternatively, the DHCP software may require creating a separate ext file with the configuration file name and path in a specific directory on the server. Consult the documentation for the DHCP server software if users are unsure.

Example usage:

To enable auto configuration on the Switch:

```
DES-3200-28:4#enable autoconfig
Command: enable autoconfig

Success.

DES-3200-28:4#
```

When autoconfig is enabled and the Switch is rebooted, the normal login screen will appear for a few moments while the autoconfig request (i.e. download configuration) is initiated. The console will then display the configuration parameters as they are loaded from the configuration file specified in the DHCP or TFTP server. This is exactly the same as using a download configuration command. After the entire Switch configuration is loaded, the Switch will automatically “logout” the server. The configuration settings will be saved automatically and become the active configuration.

Upon booting up the autoconfig process is initiated, the console screen will appear similar to the example below. The configuration settings will be loaded in normal order.


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

Firmware: Build 1.28.005
Copyright(C) 2010 D-Link Corporation. All rights reserved.

DES-3200-28:4#
DES-3200-28:4#
DES-3200-28:4#download cfg_fromTFTP 10.41.44.44 c:\cfg\setting.txt
Command: download cfg_fromTFTP 10.41.44.44 c:\cfg\setting.txt

Connecting to server..... Done.
Download configuration..... Done.
```

The very end of the autoconfig process appears like this:

```
Success.

DES-3200-28:4#
DES-3200-28:4## ROUTE
DES-3200-28:4#
DES-3200-28:4#
DES-3200-28:4##-----
DES-3200-28:4##      End of configuration file for DES-3200-28
DES-3200-28:4##-----
DES-3200-28:4#
DES-3200-28:4#
```



Note: With autoconfig enabled, the Switch ipif settings now define the Switch as a DHCP client. Use the show switch command to display the new IP settings status.

disable autoconfig

Purpose	Use this to deactivate auto configuration from DHCP.
Syntax	disable autoconfig
Description	This command is used to instruct the Switch not to accept auto configuration instruction from the DHCP server. This does not change the IP settings of the Switch. The ipif settings will continue as DHCP client until changed with the config ipif command.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To stop the auto configuration function:

```
DES-3200-28:4#disable autoconfig
Command: disable autoconfig

Success.

DES-3200-28:4#
```

show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	show autoconfig
Description	This command is used to list the current status of the auto configuration function.
Parameters	None.
Restrictions	None.

Example usage:

To display the autoconfig status:

```
DES-3200-28:4#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled
Timeout           : 50 sec

DES-3200-28:4#
```

ping	
Purpose	Used to test the connectivity between network devices.
Syntax	ping <ipaddr> {times <value 0-255>} {size <value 1-60000>} {timeout <sec 1-99>}
Description	The command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters	<p><ipaddr> – Specifies the IP address of the host.</p> <p>times <value 0-255> – 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.</p> <p>size <value 1-60000> – The size of the test packet. The value is between 1 and 60000.</p> <p>timeout <sec 1-99> – 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.</p>
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DES-3200-28:4#ping 10.48.74.121 times 4
Command: ping 10.48.74.121

Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms

Ping statistics for 10.48.74.121
Packets: Sent =4, Received =4, Lost =0

DES-3200-28:4#
```

ping6

Purpose	Used to diagnose the IPv6 network.
Syntax	ping6 <ipv6addr> {times <value 1-255> size <value 1-6000> timeout <value 1-10>}
Description	This command is used to diagnose the IPv6 network.
Parameters	<p><ipv6addr> – Specifies the IPv6 address of the host.</p> <p>times <value 1-255> – The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 1.</p> <p>size <value 1-6000> – The size of the test packet. The value is between 1 and 6000.</p> <p>timeout <value 1-10> – Defines the time-out period while waiting for a response from the remote device. A value of 1 to 10 seconds can be specified. The default is 1 second.</p>
Restrictions	None.

Example usage:

To ping the IPv6 address “FE80::254:85FF:FE32:1804” six times:

```
DES-3200-28:4#ping6 FE80::254:85FF:FE32:1804%System times 6
Command: ping6 FE80::254:85FF:FE32:1804%System times 6

Reply from FE80::254:85FF:FE32:1804, bytes=100 time=10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
Reply from FE80::254:85FF:FE32:1804, bytes=100 time<10 ms
  Ping Statistics for FE80::254:85FF:FE32:1804
    Packets: Sent =6, Received =6, Lost =0
Success.

DES-3200-28:4#
```

traceroute

Purpose	Used to trace the routed path between the Switch and a destination endstation.
Syntax	traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}
Description	This command is used to trace the routed path between the Switch and a destination endstation.
Parameters	<p><ipaddr> - The IP address of the destination endstation.</p> <p>ttl <value 1-60> - The time-to-live value of the trace route request. This is the maximum number of routers. This command will cross while seeking the network path between two devices.</p> <p>port <value 30000-64900> - The port number. It must be above 1024. The value range is between 30000 and 64900.</p> <p>probe <value 1-9> - The number of probes. The range is from 1 to 9.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To trace the routed path between the Switch and 10.48.74.121:

```
DES-3200-28:4#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

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

DES-3200-28:4#
```

config terminal line

Purpose	Used to configure the number of rows which can be displayed at a screen.
Syntax	config terminal_line [default <value 20-80>]
Description	This command is used to configure the number of rows which can be displayed on a screen. The default value is 24.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the terminal line:

```
DES-3200-28:4# config terminal_line 30
Command: config terminal_line 30

Success.

DES-3200-28:4#
```

show terminal line

Purpose	Used to display the number of rows which can be displayed at a screen.
Syntax	show terminal_line
Description	This command is used to display the number of rows which can be displayed on a screen.
Parameters	None.
Restrictions	None.

Example usage:

To show the terminal line:

```
DES-3200-28:4# show terminal_line
Command: show terminal_line

Current terminal line number : 30

DES-3200-28:4#
```

NETWORK MONITORING COMMANDS

The Network Monitoring commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[cpu dram flash ports {<portlist>}]
clear counters	{ports <portlist>}
clear log	
show log	{index <value_list X-Y>}
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> {severity [informational warning all] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <udp_port_number> ipaddress [<ipaddr>] state [enable disable] }
config syslog	{host [all <index 1-4>]} {severity [informational warning all] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <udp_port_number> ipaddress [<ipaddr>] state [enable disable]}
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	
delete ipif	[System] [ipv6address <ipv6networkaddr>]
enable ipif_ipv6_link_local_auto	[System]
disable ipif_ipv6_link_local_auto	[System]
show ipif_ipv6_link_local_auto	

Each command is listed, in detail, in the following sections:

show packet ports

Purpose	Used to display stats about packets sent and received by the Switch.
Syntax	show packet ports <portlist>
Description	This command is used to display statistics about packets sent and received by ports specified in the <portlist>.
Parameters	<portlist> – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the packets analysis for port 2:

```
DES-3200-28:4#show packet ports 2
Command: show packet ports 2

Port Number : 2

```

Frame Size	Frame Counts	Frames/sec	Frame Type	Total	Total/sec
-----	-----	-----	-----	-----	-----
64	0	0	RX Bytes	0	0
65-127	0	0	RX Frames	0	0
128-255	0	0			
256-511	0	0	TX Bytes	0	0
512-1023	0	0	TX Frames	0	0
1024-1518	0	0			
Unicast RX	0	0			
Multicast RX	0	0			
Broadcast RX	0	0			

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


show error ports

Purpose	Used to display the error statistics for a range of ports.
Syntax	show error ports <portlist>
Description	This command is used to display all of the packet error statistics collected and logged by the Switch for a given port list.
Parameters	<portlist> – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the errors of the port 3:

```
DES-3200-28:4#show error ports 3
Command: show error ports 3

Port Number : 3

          RX Frames                                TX Frames
          -----                                -----
CRC Error      0                                Excessive Deferral  0
Undersize     0                                CRC Error            0
Oversize      0                                Late Collision       0
Fragment      0                                Excessive Collision  0
Jabber        0                                Single Collision     0
Drop Pkts     0                                Collision            0

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

show utilization	
Purpose	Used to display real-time utilization statistics.
Syntax	show utilization [cpu dram flash ports {<portlist>}]
Description	This command is used to display the real-time utilization statistics for the Switch.
Parameters	<p>cpu – Entering this parameter will display the current CPU utilization of the Switch.</p> <p>dram – Entering this parameter will display the current DRAM utilization of the Switch.</p> <p>flash – Entering this parameter will display the current Flash utilization of the Switch.</p> <p>ports – Entering this parameter will display the current port utilization of the Switch.</p> <p><portlist> – Specifies a range of ports to be displayed.</p>
Restrictions	None.

Example usage:

To display the current CPU utilization:

```
DES-3200-28:4#show utilization cpu
Command: show utilization cpu

CPU Utilization :
-----
Five Seconds - 3%      One Minute - 2%      Five Minutes - 5%

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

To display the current DRAM utilization:

```
DES-3200-28:4#show utilization dram
Command: show utilization dram

DRAM Utilization :

Total DRAM      : 131,072   KB
Used DRAM       : 65,604    KB
Utilization     : 50%

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

To display the current Flash memory utilization:

```
DES-3200-28:4#show utilization flash
Command: show utilization flash

FLASH Memory Utilization :

Total FLASH      : 16,384    KB
Used FLASH       : 7,371     KB
Utilization      : 44%

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

To display the port utilization statistics:

```
DES-3200-28:4#show utilization ports
Command: show utilization ports
```

Port	Tx/sec	Rx/sec	Util	Port	Tx/sec	Rx/sec	Util
1	0	0	0	22	0	0	0
2	0	0	0	23	0	0	0
3	0	0	0	24	0	0	0
4	0	0	0	25	0	0	0
5	0	0	0	26	0	0	0
6	0	0	0	27	0	0	0
7	0	37	1	28	0	0	0
8	0	0	0				
9	0	0	0				
10	0	0	0				
11	36	0	1				
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				
21	0	0	0				

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

clear counters

Purpose	Used to clear the Switch's statistics counters.
Syntax	clear counters {ports <portlist>}
Description	This command is used to clear the counters used by the Switch to compile statistics.
Parameters	<portlist> – Specifies a port or range of ports to be displayed.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear the counters:

```
DES-3200-28:4#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

DES-3200-28:4#
```

clear log

Purpose	Used to clear the Switch's history log.
Syntax	clear log
Description	This command is used to clear the Switch's history log.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear the log information:

```
DES-3200-28:4#clear log
Command: clear log

Success.

DES-3200-28:4#
```

show log

Purpose	Used to display the switch history log.
Syntax	show log {index <value_list X-Y>}
Description	This command is used to display the contents of the Switch's history log.
Parameters	index <value_list X-Y> – This command will display the history log, beginning and ending at the value specified by the user in the <value_list X-Y> field. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.

Example usage:

To display the switch history log:

```
DES-3200-28:4#show log index 1-5
Command: show log index 1-5

Index  Data          Time          Log Text
-----  -
5      00000-00-00 01:01:09 Successful login through Console (Username: Anonymous)
4      00000-00-00 00:00:14 System warm start
3      00000-00-00 00:00:06 Port 25 link up, 1000Mbps FULL duplex
2      00000-00-00 00:00:01 Port 25 link down
1      00000-00-00 00:06:31 Port 25 link up, 1000Mbps FULL duplex

DES-3200-28:4#
```

enable syslog

Purpose	Used to enable the system log to be sent to a remote host.
Syntax	enable syslog
Description	This command is used to enable the system log to be sent to a remote host.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the syslog function on the Switch:

```
DES-3200-28:4#enable syslog
Command: enable syslog

Success.

DES-3200-28:4#
```

disable syslog

Purpose	Used to disable the system log to be sent to a remote host.
Syntax	disable syslog

disable syslog

Description	This command is used to disable the system log to be sent to a remote host.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DES-3200-28:4#disable syslog
Command: disable syslog

Success.

DES-3200-28:4#
```

show syslog

Purpose	Used to display the syslog protocol status as enabled or disabled.
Syntax	show syslog
Description	This command is used to display the syslog status as enabled or disabled.
Parameters	None.
Restrictions	None.

Example usage:

To display the current status of the syslog function:

```
DES-3200-28:4#show syslog
Command: show syslog

Syslog Global State : Disabled

DES-3200-28:4#
```

create syslog host																					
Purpose	Used to create a new syslog host.																				
Syntax	create syslog host <index 1-4> {severity [informational warning all] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <udp_port_number> ipaddress [<ipaddr>] state [enable disable] }																				
Description	This command is used to create a new syslog host.																				
Parameters	<p><index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p>severity – Severity level indicator. These are described in the following: Bold font indicates that the corresponding severity level is currently supported on the Switch.</p> <table border="1"> <thead> <tr> <th>Numerical Code</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency: system is unusable</td> </tr> <tr> <td>1</td> <td>Alert: action must be taken immediately</td> </tr> <tr> <td>2</td> <td>Critical: critical conditions</td> </tr> <tr> <td>3</td> <td>Error: error conditions</td> </tr> <tr> <td>4</td> <td>Warning: warning conditions</td> </tr> <tr> <td>5</td> <td>Notice: normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational: informational messages</td> </tr> <tr> <td>7</td> <td>Debug: debug-level messages</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Numerical Code</th> <th>Facility</th> </tr> </thead> <tbody> </tbody> </table>	Numerical Code	Severity	0	Emergency: system is unusable	1	Alert: action must be taken immediately	2	Critical: critical conditions	3	Error: error conditions	4	Warning: warning conditions	5	Notice: normal but significant condition	6	Informational: informational messages	7	Debug: debug-level messages	Numerical Code	Facility
Numerical Code	Severity																				
0	Emergency: system is unusable																				
1	Alert: action must be taken immediately																				
2	Critical: critical conditions																				
3	Error: error conditions																				
4	Warning: warning conditions																				
5	Notice: normal but significant condition																				
6	Informational: informational messages																				
7	Debug: debug-level messages																				
Numerical Code	Facility																				

create syslog host

0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

local0 – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above.

local1 – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above.

local2 – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above.

local3 – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.

local4 – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.

local5 – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.

local6 – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.

local7 – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.

udp_port <udp_port_number> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.

ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent.

state [enable | disable] – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To create a syslog host:


```
DES-3200-28:4#create syslog host 1 ipaddress 10.68.88.1 severity all facility local0
Command: create syslog host 1 ipaddress 10.68.88.1 severity all facility local0

Success.

DES-3200-28:4#
```

config syslog																			
Purpose	Used to configure the syslog protocol to send system log data to a remote host.																		
Syntax	config syslog {host [all <index 1-4>]} {severity [informational warning all] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <udp_port_number> ipaddress [<ipaddr>] state [enable disable] }																		
Description	This command is used to configure the syslog protocol to send system log information to a remote host.																		
Parameters	<p>all – This is to specify all available indexes.</p> <p><index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p>severity – Severity level indicator. These are described in the following: Bold font indicates that the corresponding severity level is currently supported on the Switch.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Numerical Code</th> <th style="text-align: left;">Severity</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency: system is unusable</td> </tr> <tr> <td>1</td> <td>Alert: action must be taken immediately</td> </tr> <tr> <td>2</td> <td>Critical: critical conditions</td> </tr> <tr> <td>3</td> <td>Error: error conditions</td> </tr> <tr> <td>4</td> <td>Warning: warning conditions</td> </tr> <tr> <td>5</td> <td>Notice: normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational: informational messages</td> </tr> <tr> <td>7</td> <td>Debug: debug-level messages</td> </tr> </tbody> </table> <p>informational – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above.</p> <p>warning – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above.</p> <p>all – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host.</p> <p>facility – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font indicates the facility values the Switch currently supports.</p>	Numerical Code	Severity	0	Emergency: system is unusable	1	Alert: action must be taken immediately	2	Critical: critical conditions	3	Error: error conditions	4	Warning: warning conditions	5	Notice: normal but significant condition	6	Informational: informational messages	7	Debug: debug-level messages
Numerical Code	Severity																		
0	Emergency: system is unusable																		
1	Alert: action must be taken immediately																		
2	Critical: critical conditions																		
3	Error: error conditions																		
4	Warning: warning conditions																		
5	Notice: normal but significant condition																		
6	Informational: informational messages																		
7	Debug: debug-level messages																		

Parameters	Numerical Code	Facility
	0	kernel messages
	1	user-level messages
	2	mail system
	3	system daemons
	4	security/authorization messages
	5	messages generated internally by syslog
	6	line printer subsystem
	7	network news subsystem
	8	UUCP subsystem
	9	clock daemon
	10	security/authorization messages
	11	FTP daemon
	12	NTP subsystem
	13	log audit
	14	log alert
	15	clock daemon
	16	local use 0 (local0)
	17	local use 1 (local1)
	18	local use 2 (local2)
	19	local use 3 (local3)
	20	local use 4 (local4)
	21	local use 5 (local5)
	22	local use 6 (local6)
	23	local use 7 (local7)
	<p>local0 – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above.</p> <p>local1 – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above.</p> <p>local2 – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above.</p> <p>local3 – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.</p> <p>local4 – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.</p> <p>local5 – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.</p> <p>local6 – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.</p> <p>local7 – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.</p> <p>udp_port <udp_port_number> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.</p> <p>ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent.</p> <p>state [enable disable] – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.</p>	
Restrictions	Only Administrator-level users can issue this command.	

Example usage:

To configure a syslog host:

```
DES-3200-28:4#config syslog host 1 severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DES-3200-28:4#
```

To configure a syslog host for all hosts:

```
DES-3200-28:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DES-3200-28:4#
```

delete syslog host

Purpose	Used to remove a syslog host that has been previously configured, from the Switch.
Syntax	delete syslog host [<index 1-4> all]
Description	This command is used to remove a syslog host that has been previously configured from the Switch.
Parameters	<index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. all – Specifies that the command will be applied to all hosts.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DES-3200-28:4#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3200-28:4#
```

show syslog host

Purpose	Used to display the syslog hosts currently configured on the Switch.
Syntax	show syslog host {<index 1-4>}
Description	This command is used to display the syslog hosts that are currently configured on the Switch.
Parameters	<index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.
Restrictions	None.

Example usage:

To show syslog host information:

```
DES-3200-28:4#show syslog host
Command: show syslog host

Syslog Global State: Disabled

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

Total Entries : 3

DES-3200-28:4#
```

config log_save_timing

Purpose	Used to configure the method of saving logs to the Switch's Flash memory.
Syntax	config log_save_timing [time_interval <min 1-65535> on_demand log_trigger]
Description	This command is used to configure the method used in saving logs to the Switch's Flash memory.
Parameters	<p>time_interval <min 1-65535> – Use this parameter to configure the time interval that will be implemented for saving logs. The logs will be saved every x number of minutes that are configured here.</p> <p>on_demand – Users who choose this method will only save logs when they manually tell the Switch to do so, using the save all or save log command.</p> <p>log_trigger – Users who choose this method will have logs saved to the Switch every time a log event occurs on the Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the time interval as every 30 minutes for saving logs:

```
DES-3200-28:4#config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

DES-3200-28:4#
```

show log_save_timing

Purpose	Used to display the method configured for saving logs to the Switch's Flash memory.
Syntax	show log_save_timing
Description	This command is used to view the method configured for saving logs to the Switch's Flash memory.
Parameters	None.
Restrictions	None.

Example usage:

To display the method for saving logs:

```
DES-3200-28:4#show log_save_timing
Command: show log_save_timing

Saving log method: on_demand

DES-3200-28:4#
```

delete ipif

Purpose	Used to delete an interface.
Syntax	delete ipif [System] [ipv6address <ipv6networkaddr>]
Description	This command is used to delete an interface. The System interface cannot be deleted. By using this command, an IPv6 address can be deleted from the ipif.
Parameters	<ipv6networkaddr> – Specifies the IPv6 network address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an IPv6 address of the System interface:

```
DES-3200-28:4#delete ipif System ipv6address FE80::200:1FF:FE02:303/128
Command: delete ipif System ipv6address FE80::200:1FF:FE02:303/128

Success.

DES-3200-28:4#
```

enable ipif_ipv6_link_local_auto

Purpose	Used to enable the auto configuration of a link local address when no IPv6 address is configured.
Syntax	enable ipif_ipv6_link_local_auto [System]
Description	This command is used to enable the auto configuration of a 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 start. When there is no IPv6 address explicitly configured, by default, a link local address is not configured and the IPv6 processing will be disabled. By enabling this automatic configuration, the link local address will be automatically configured and the IPv6 processing will start.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the automatic configuration of a link local address for an interface:

```
DES-3200-28:4#enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System

Success.

DES-3200-28:4#
```

disable ipif_ipv6_link_local_auto

Purpose	Used to disable the auto configuration of a link local address when no IPv6 address is configured.
Syntax	disable ipif_ipv6_link_local_auto [System]
Description	This command is used to disable the auto configuration of a link local address when no IPv6 address is explicitly configured.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the automatic configuration of link local address for an interface:

```
DES-3200-28:4#disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success.

DES-3200-28:4#
```

show ipif_ipv6_link_local_auto

Purpose	Used to display the link local address automatic configuration state.
Syntax	show ipif_ipv6_link_local_auto
Description	This command is used to display the link local address automatic configuration state.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display interface information:

```
DES-3200-28:4#show pif_ipv6_link_local_auto
Command: show pif_ipv6_link_local_auto

IPIF: System          Automatic Link Local Address: Disabled
DES-3200-28:4#
```

MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS

This Switch supports three versions of the Spanning Tree Protocol; 802.1D STP, 802.1w Rapid STP and 802.1s MSTP. Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing either of the three spanning tree protocols (STP, RSTP or MSTP). This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. These instances will be classified by an instance_id. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees. Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

A configuration name defined by an alphanumeric string of up to 32 characters (defined in the `config stp mst_config_id` command as `name <string>`).

A configuration revision number (named here as a `revision_level`) and;

A 4094 element table (defined here as a `vid_range`) which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

The Switch must be set to the MSTP setting (`config stp version`)

The correct spanning tree priority for the MSTP instance must be entered (`config stp priority`).

VLANs that will be shared must be added to the MSTP Instance ID (`config stp instance_id`).

The Multiple Spanning Tree Protocol commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

enable stp	
disable stp	
config stp version	[mstp rstp stp]
config stp	{maxage <value 6-40> maxhops <value 6-40> hellotime <value 1-2> forwarddelay <value 4-30> txholdcount <value 1-10> fbpdudisable [enable disable]} (1)
config stp ports	<portlist> {externalCost [auto <value 1-200000000>] hellotime <value 1-2> migrate [yes no] edge [true false auto] restricted_role [true false] restricted_tcn [true false] p2p [true false auto] state [enable disable] fbpdudisable [enable disable]} (1)
create stp instance_id	<value 1-8>
config stp instance_id	<value 1-8> [add_vlan remove_vlan] <vidlist>
delete stp instance_id	<value 1-8>
config stp priority	<value 0-61440> instance_id <value 0-8>
config stp mst_config_id	{revision_level <int 0-65535> name <string>} (1)
config stp mst_ports	<portlist> instance_id <value 0-8> {internalCost [auto <value 1-200000000>] priority <value 0-240>} (1)
show stp	
show stp ports	{<portlist>} {instance <value 0-8>}
show stp instance	{<value 0-8>}
show stp mst_config id	

Each command is listed, in detail, in the following sections:

enable stp

Purpose	Used to globally enable STP on the Switch.
Syntax	enable stp
Description	This command is used to globally enable the Spanning Tree Protocol on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DES-3200-28:4#enable stp
Command: enable stp

Success.

DES-3200-28:4#
```

disable stp

Purpose	Used to globally disable STP on the Switch.
Syntax	disable stp
Description	This command is used to globally disable the Spanning Tree Protocol on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DES-3200-28:4#disable stp
Command: disable stp

Success.

DES-3200-28:4#
```

config stp version

Purpose	Used to globally set the version of STP on the Switch.
Syntax	config stp version [mstp rstp stp]
Description	This command is used to choose the version of the spanning tree to be implemented on the Switch.
Parameters	mstp – Selecting this parameter will set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. rstp – Selecting this parameter will set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. stp – Selecting this parameter will set the Spanning Tree Protocol (STP) globally on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:


To set the Switch globally for the Multiple Spanning Tree Protocol (MSTP):

```
DES-3200-28:4#config stp version mstp
Command: config stp version mstp

Success.

DES-3200-28:4#
```

config stp

Purpose	Used to set up STP, RSTP, and MSTP on the Switch.
Syntax	<code>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] } (1)</code>
Description	This command is used to set up the Spanning Tree Protocol (STP) for the entire Switch. All commands here will be implemented for the STP version that is currently set on the Switch.
Parameters	<p><code>maxage <value 6-40></code> – This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20.</p> <p><code>maxhops <value 6-40></code> – The number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 6 to 40. The default is 20.</p> <p><code>hellotime <value 1-2></code> – The user may set the time interval between transmission of configuration messages by the root device, thus stating that the Switch is still functioning. A time between 1 and 2 seconds may be chosen, with a default setting of 2 seconds.</p> <p> NOTE: In MSTP, the spanning tree is configured by port and therefore, the hellotime must be set using the <code>configure stp ports</code> command for switches utilizing the Multiple Spanning Tree Protocol.</p> <p><code>forwarddelay <value 4-30></code> – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds.</p> <p><code>txholdcount <value 1-10></code> – The maximum number of BPDU Hello packets transmitted per interval. The default value is 6.</p> <p><code>fbpdu [enable disable]</code> – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is enable.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DES-3200-28:4#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

DES-3200-28:4#
```

config stp ports

Purpose	Used to set up STP on the port level.
Syntax	config stp ports <portlist> {externalCost [auto <value 1-200000000>] hellotime <value 1-2> migrate [yes no] edge [true false auto] restricted_role [true false] restricted_tcn [true false] p2p [true false auto] state [enable disable] fbpdu [enable disable] } (1)
Description	This command is used to create and configure STP for a group of ports.
Parameters	<p><portlist> – Specifies a range of ports to be configured.</p> <p>externalCost – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is auto.</p> <p>auto – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.</p> <p><value 1-200000000> – Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.</p> <p>hellotime <value 1-2> – The time interval between transmission of configuration messages by the designated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and 2 seconds. The default is 2 seconds.</p> <p>migrate [yes no] – Setting this parameter as “yes” will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1D STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1D network connects to an 802.1w or 802.1s enabled network. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment.</p> <p>edge [true false auto] – true designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. false indicates that the port does not have edge port status.</p> <p>p2p [true false auto] – true indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. Auto allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were false. The default setting for this parameter is auto.</p> <p>state [enable disable] – Allows STP to be enabled or disabled for the ports specified in the port list. The default is enable.</p> <p>restricted_role – To decide if this is to be selected as the Root Port. The default value is false.</p> <p>restricted_tcn – To decide if this port is to propagate topology change. The default value is false.</p> <p>fbpdu [enable disable] – When enabled, this allows the forwarding of STP BPDU packets from other network devices when STP is disabled in the specified ports. If users want to enable Forwarding BPDU on a per port basis, the following settings must first be in effect: 1. STP must be globally disabled and 2. Forwarding BPDU must be globally enabled. To globally disable STP, use the disable stp command, to globally enable fbpdu, use the config stp command. The default is enable.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure STP with path cost auto, hellotime 2 seconds, migration enable, and state enable for ports 1 to 2:

```
DES-3200-28:4#config stp ports 1-2 externalCost auto hellotime 2 migrate yes state enable
Command: config stp ports 1-2 externalCost auto hellotime 2 migrate yes state enable

DES-3200-28:4#
```

create stp instance_id

Purpose	Used to create a STP instance ID for MSTP.
Syntax	create stp instance_id <value 1-8>
Description	This command allows the user to create a STP instance ID for the Multiple Spanning Tree Protocol. There are five STP instances on the Switch (one internal CIST, unchangeable) and the user may create up to four instance IDs for the Switch.
Parameters	<value 1-8> – Enter a value between 1 and 8 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:


To create a spanning tree instance 2:

```
DES-3200-28:4#create stp instance_id 2
Command: create stp instance_id 2

Success.

DES-3200-28:4#
```

config stp instance_id

Purpose	Used to add or delete an STP instance ID.
Syntax	config stp instance_id <value 1-8> [add_vlan remove_vlan] <vidlist>
Description	<p>This command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an instance_id. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of five spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time.</p> <div style="display: flex; align-items: center;">  <p>Note: Switches in the same spanning tree region having the same STP instance_id must be mapped identically, and have the same configuration revision_level number and the same name.</p> </div>
Parameters	<p><value 1-8> – Enter a number between 1 and 8 to define the instance_id. The Switch supports five STP instances with one unchangeable default instance ID set as 0.</p> <p>add_vlan – Along with the vid_range <vidlist> parameter, this command will add VIDs to the previously configured STP instance_id.</p> <p>remove_vlan – Along with the vid_range <vidlist> parameter, this command will remove VIDs to the previously configured STP instance_id.</p> <p><vidlist> – Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DES-3200-28:4#config stp instance_id 2 add_vlan 10
Command: config stp instance_id 2 add_vlan 10

Success.

DES-3200-28:4#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DES-3200-28:4#config stp instance_id 2 remove_vlan 10
Command: config stp instance_id 2 remove_vlan 10

Success.

DES-3200-28:4#
```

delete stp instance_id

Purpose	Used to delete a STP instance ID from the Switch.
Syntax	delete stp instance_id <value 1-8>
Description	This command is used to delete a previously configured STP instance ID from the Switch.
Parameters	<value 1-8> – Enter a value between 1 and 8 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete STP instance ID 2 from the Switch.

```
DES-3200-28:4#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DES-3200-28:4#
```

config stp priority

Purpose	Used to update the STP instance configuration
Syntax	config stp priority <value 0-61440> instance_id <value 0-8>
Description	This command is used to update the STP instance configuration settings on the Switch. The MSTP will utilize the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions will instruct the Switch to give precedence to the selected instance_id for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	priority <value 0-61440> – Select a value between 0 and 61440 to specify the priority for a specified instance ID for forwarding packets. The lower the value, the higher the priority. This entry must be divisible by 4096. instance_id <value 0-8> – Enter the value corresponding to the previously configured instance ID of which the user wishes to set the priority value. An instance id of 0 denotes the default instance_id (CIST) internally set on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the priority value for instance_id 2 as 4096:

```
DES-3200-28:4#config stp priority 4096 instance_id 2
Command: config stp priority 4096 instance_id 2

Success.

DES-3200-28:4#
```


config stp mst_config_id

Purpose	Used to update the MSTP configuration identification.
Syntax	config stp mst_config_id {revision_level <int 0-65535> name <string>}
Description	This command is used to uniquely identify the MSTP configuration currently configured on the Switch. Information entered here will be attached to BPDU packets as an identifier for the MSTP region to which it belongs. Switches having the same revision_level and name will be considered as part of the same MSTP region.
Parameters	<p>revision_level <int 0-65535> – Enter a number between 0 and 65535 to identify the MSTP region. This value, along with the name will identify the MSTP region configured on the Switch. The default setting is 0.</p> <p>name <string> – Enter an alphanumeric string of up to 32 characters to uniquely identify the MSTP region on the Switch. This name, along with the revision_level value will identify the MSTP region configured on the Switch. If no name is entered, the default name will be the MAC address of the device.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the MSTP region of the Switch with revision level 10 and the name “DLee”:

```
DES-3200-28:4#config stp mst_config_id revision_level 10 name DLee
Command: config stp mst_config_id revision_level 10 name DLee

Success.

DES-3200-28:4#
```

config stp mst_ports

Purpose	Used to update the port configuration for a MSTP instance.
Syntax	config stp mst_ports <portlist> instance_id <value 0-8> {internalCost [auto <value 1-200000000>] priority <value 0-240>} (1)
Description	This command is used to update the port configuration for a STP instance_id. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p>instance_id <value 0-8> – Enter a numerical value between 0 and 8 to identify the instance_id previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree).</p> <p>internalCost – This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is auto. There are two options:</p> <p>auto – Selecting this parameter for the internalCost will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.</p> <p>value 1-200000000 – Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower internalCost represents a quicker transmission.</p> <p>priority <value 0-240> – Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To designate ports 1 through 5, with instance id 2, to have an auto internalCost and a priority of 16:

```
DES-3200-28:4#config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16
Command : config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16

Success.

DES-3200-28:4#
```

show stp

Purpose	Used to display the Switch's current STP configuration.
Syntax	show stp
Description	This command is used to display the Switch's current STP configuration.
Parameters	None
Restrictions	None.

Example usage:

To display the status of STP on the Switch:

Status 1: STP enabled with STP compatible version

```
DES-3200-28:4#show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status      : Enabled
STP Version     : STP compatible
Max Age        : 20
Hello Time     : 2
Forward Delay  : 15
Max Hops       : 20
TX Hold Count  : 6
Forwarding BPDU : Enabled

DES-3200-28:4#
```

Status 2 : STP enabled for RSTP

```
DES-3200-28:4#show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status      : Enabled
STP Version     : RSTP
Max Age         : 20
Hello Time      : 2
Forward Delay   : 15
Max Hops        : 20
TX Hold Count   : 6
Forwarding BPDU : Enabled

DES-3200-28:4#
```

Status 3 : STP enabled for MSTP

```
DES-3200-28:4#show stp
Command: show stp
STP Bridge Global Settings
-----
STP Status      : Enabled
STP Version     : MSTP
Max Age         : 20
Forward Delay   : 15
Max Hops        : 20
TX Hold Count   : 6
Forwarding BPDU : Enabled

DES-3200-28:4#
```

show stp ports

Purpose	Used to display the Switch's current STP ports configuration.
Syntax	show stp ports {<portlist>} {instance <value 0-8>}
Description	This command is used to display the STP port settings for a specified port or group of ports.
Parameters	<p><portlist> – Specifies a port or range of ports to be viewed. Information for a single port is displayed. If no ports are specified the STP information for port 1 will be displayed. Users may use the Space bar, p and n keys to view information for the remaining ports.</p> <p>instance <value 0-8> – Enter a value between 0 and 8 corresponding to the previously configured instance_id of which the user wishes to show the specified ports' setting. An instance id of 0 denotes the default instance_id (CIST) internally set on the Switch.</p>
Restrictions	None.

Example usage:

To show STP ports information for port 1 (STP enabled on Switch):

```
DES-3200-28:4#show stp ports
Command: show stp ports

MSTP Port Information
-----
Port Index      : 1      , Hello Time: 2 /2 , Port STP Enabled  ,
Restricted role  : False, Restricted TCN : False
External PathCost : Auto/200000  , Edge Port : Auto /No , P2P : Auto /Yes
Port Forward BPDU : Enabled
MSTI   Designated Bridge   Internal PathCost   Prio   Status       Role
-----
0      N/A                  200000             128    Disabled     Disabled

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

show stp instance

Purpose	Used to display the Switch's STP instance configuration
Syntax	show stp instance {<value 0-8>}
Description	This command is used to display the Switch's current STP Instance Settings and the STP Instance Operational Status.
Parameters	<value 0-8> – Enter a value defining the previously configured instance_id on the Switch. An entry of 0 will display the STP configuration for the CIST internally set on the Switch.
Restrictions	None

Example usage:

To display the STP instance configuration for instance 0 (the internal CIST) on the Switch:

```
DES-3200-28:4#show stp instance 0
Command: show stp instance 0

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 : 32766/00-90-27-39-78-E2
External Root Cost     : 200012
Regional Root Bridge  : 32768/00-53-13-1A-33-24
Internal Root Cost     : 0
Designated Bridge     : 32768/00-50-BA-71-20-D6
Root Port              : 1
Max Age                : 20
Forward Delay         : 15
Last Topology Change  : 856
Topology Changes Count : 2987

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

show stp mst_config_id

Purpose	Used to display the MSTP configuration identification.
Syntax	show stp mst_config_id
Description	This command is used to display the Switch's current MSTP configuration identification.
Parameters	None.
Restrictions	None.

Example usage:

To show the MSTP configuration identification currently set on the Switch:

```
DES-3200-28:4#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
-----

Configuration Name : 00:53:13:1A:33:24          Revision Level :0
MSTI ID           VID list
-----
      CIST             1-4094

DES-3200-28:4#
```

FORWARDING DATABASE COMMANDS

The Layer 2 Forwarding Database commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add delete] <portlist>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> port <port> all]
show multicast_fdb	{vlan <vlan_name 32> mac_address <macaddr>}
show fdb	{port <port> vlan <vlan_name 32> vlanid <vidlist> mac_address <macaddr> static aging_time}
config multicast port_filtering_mode	[<portlist> all] [forward_unregistered_groups filter_unregistered_groups]
show multicast port_filtering_mode	

Each command is listed, in detail, in the following sections:

create fdb

Purpose	Used to create a static entry in the unicast MAC address forwarding table (database).
Syntax	create fdb <vlan_name 32> <macaddr> port <port>
Description	This command is used to make an entry in the Switch's unicast MAC address forwarding database.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be added to the forwarding table.</p> <p>port <port> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a unicast MAC FDB entry:

```
DES-3200-28:4#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DES-3200-28:4#
```

create multicast_fdb

Purpose	Used to create a static entry in the multicast MAC address forwarding table (database)
Syntax	create multicast_fdb <vlan_name 32> <macaddr>
Description	This command is used to make an entry in the Switch's multicast MAC address forwarding database.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be added to the forwarding table.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a multicast MAC forwarding entry:

```
DES-3200-28:4#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DES-3200-28:4#
```

config multicast_fdb

Purpose	Used to configure the Switch's multicast MAC address forwarding database.
Syntax	config multicast_fdb <vlan_name 32> <macaddr> [add delete] <portlist>
Description	This command is used to configure the multicast MAC address forwarding table.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be added to the multicast forwarding table.</p> <p>[add delete] – add will add ports to the forwarding table. delete will remove ports from the multicast forwarding table.</p> <p><portlist> – Specifies a port or range of ports to be configured.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure multicast MAC forwarding:

```
DES-3200-28:4#config multicast_fdb default 01-00-00-00-00-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1-5

Success.

DES-3200-28:4#
```

config fdb aging_time

Purpose	Used to set the aging time of the forwarding database.
Syntax	config fdb aging_time <sec 10-1000000>
Description	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.
Parameters	<sec 10-1000000> – The aging time for the MAC address forwarding database value. The value in seconds may be between 10 and 1000000 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the fdb aging time:

```
DES-3200-28:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3200-28:4#
```

delete fdb

Purpose	Used to delete an entry to the Switch's forwarding database.
Syntax	delete fdb <vlan_name 32> <macaddr>
Description	This command is used to delete a previous entry to the Switch's MAC address forwarding database.
Parameters	<vlan_name 32> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DES-3200-28:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3200-28:4#
```

To delete a multicast FDB entry:

```
DES-3200-28:4#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DES-3200-28:4#
```

clear fdb

Purpose	Used to clear the Switch's forwarding database of all dynamically learned MAC addresses.
Syntax	clear fdb [vlan <vlan_name 32> port <port> all]
Description	This command is used to clear dynamically learned entries to the Switch's forwarding database.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p>port <port> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p> <p>all – Clears all dynamic entries to the Switch's forwarding database.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

```
DES-3200-28:4#clear fdb all
Command: clear fdb all

Success.

DES-3200-28:4#
```

show multicast_fdb

Purpose	Used to display the contents of the Switch's multicast forwarding database.
Syntax	show multicast_fdb {vlan <vlan_name 32> mac_address <macaddr>}
Description	This command is used to display the current contents of the Switch's multicast MAC address forwarding database.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – Specifies a MAC address for which FDB entries will be displayed.</p> <p>If no parameter is specified, all multicast FDB entries will be displayed.</p>
Restrictions	None.

Example usage:

To display the multicast MAC address table:

```
DES-3200-28:4#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

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

Total Entries  : 1

DES-3200-28:4#
```

show fdb	
Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	show fdb {port <port> vlan <vlan_name 32> vlandid <vidlist> mac_address <macaddr> static aging_time}
Description	This command is used to display the current contents of the Switch's forwarding database.
Parameters	port <port> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. <vlan_name 32> – The name of the VLAN on which the MAC address resides. <vidlist> – Displays the entries for the VLANs indicated by VID list. <macaddr> – The MAC address that is present in the forwarding database table. static – Displays the static MAC address entries. aging_time – Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DES-3200-28:4#show fdb
Command: show fdb

Unicast MAC Address Ageing Time = 300

VID  VLAN Name                MAC Address          Port Type
-----
1    default                    00-00-51-43-70-00  CPU    Self

Total Entries   : 1

DES-3200-28:4#
```

config multicast port_filtering_mode	
Purpose	Used to configure the multicast packet filtering mode for ports.
Syntax	config multicast port_filtering_mode [<portlist> all] [forward_unregistered_groups filter_unregistered_groups]
Description	This command is used to configure the multicast packet filtering mode for specified ports on the Switch.
Parameters	[<portlist> all] – Enter a port or list of ports for which to configure the multicast port filtering mode. Entering the all parameter will denote all ports on the switch. [forward_unregistered_groups filter_unregistered_groups] – The user may set the filtering mode to any of these two options.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the multicast filtering mode to forward all groups on ports 1 through 4.

```
DES-3200-28:4#config      multicast      port_filtering_mode      1-4
forward_unregistered_groups
Command:      config      multicast      port_filtering_mode      1-4
forward_unregistered_groups

Success.

DES-3200-28:4#
```

show multicast port_filtering_mode

Purpose	Used to show the multicast packet filtering mode for ports.
Syntax	show multicast port_filtering_mode
Description	This command is used to display the current multicast packet filtering mode for ports on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the multicast port filtering mode for all ports:

```
DES-3200-28:4#show multicast port_filtering_mode
Command: show multicast port_filtering_mode

Multicast Filter Mode For Unregistered Group:
    Forwarding List: 1-28
    Filtering List:

DES-3200-28:4#
```

PACKET STORM CONTROL COMMANDS

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase due to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the Drop option of the Action field in the table below. The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the Countdown field. If this field times out and the packet storm continues, the port will be placed in a Rest mode which will produce a warning message to be sent to the Trap Receiver. Once in Rest mode, the only methods of recovering this port are (1) auto-recovery after 5 minutes or (2) to manually recoup it using the Port Configuration window in the Administration folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the Shutdown option of the Action field in the table below.

The Packet Storm Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config traffic control	[<portlist> all] {broadcast [enable disable] multicast [enable disable] unicast [enable disable] action [drop shutdown] threshold <value 64-1000000> time_interval <secs 5-30> countdown [<minutes 0> <minutes 5-30>] } (1)
show traffic control	{<portlist>}
config traffic control_trap	[none storm_occurred storm_cleared both]

Each command is listed, in detail, in the following sections:

config traffic control

Purpose	Used to configure broadcast/multicast/unicast packet storm control. The software mechanism is provided to monitor the traffic rate in addition to the hardware storm control mechanism previously provided.
Syntax	[<portlist> all] {broadcast [enable disable] multicast [enable disable] unicast [enable disable] action [drop shutdown] threshold <value 64-1000000> time_interval <secs 5-30> countdown [<minutes 0> <minutes 5-30>] } (1)
Description	This command is used to configure broadcast/multicast/unicast storm control. By adding the new software traffic control mechanism, the user can now use both a hardware and software mechanism, the latter of which will now provide shutdown, recovery and trap notification functions for the Switch.
Parameters	<p><portlist> – Used to specify a range of ports to be configured for traffic control.</p> <p>all – Specifies all ports are to be configured for traffic control on the Switch.</p> <p>broadcast [enable disable] – Enables or disables broadcast storm control.</p> <p>multicast [enable disable] – Enables or disables multicast storm control.</p> <p>unicast [enable disable] – Enables or disables Unknown unicast traffic control.</p> <p>action – Used to configure the action taken when a storm control has been detected on the Switch. The user has two options:</p> <ul style="list-style-type: none"> drop – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. shutdown – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Storm continues, the port will be placed in Rest mode and is no longer operational until (1) auto-recovery after 5 minutes or (2) the user manually resets the port using the config ports 1 state disable and config ports 1 state enable command. Choosing this option obligates the user to configure the time_interval field as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring. <p>threshold <value 64-1000000> – This value represents the upper threshold at which the specified traffic control is switched on. The threshold value is measured in Kbit/sec when the action is set to drop mode; it is measured in pps(packets/sec) when the action is set to shutdown mode. That is, the number of broadcast/multicast/Unknown unicast packets, received by the Switch that will trigger the storm traffic control measures.</p> <p>The default setting is 64 Kbit/sec.</p> <p>time_interval – The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value.</p> <p>countdown – The countdown timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as shutdown in the action field of this command and therefore will not operate for Hardware based Traffic Control implementations.</p> <ul style="list-style-type: none"> <minutes 0> – 0 is the default setting for this field and 0 will denote that the port will never shutdown. <minutes 5-30> – Select a time from 5 to 30 minutes that the Switch will wait before shutting down. Once this time expires and the port is still experiencing packet storms, the port will be placed in rest mode and can only be manually recovered using the config ports command mentioned previously in this manual. <secs 5-30> – The Interval may be set between 5 and 30 seconds with the default setting of 5 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure traffic control and enable broadcast storm control for ports 1 to 12:

```
DES-3200-28:4#config traffic control 1-12 broadcast enable action shutdown
threshold 64 countdown 10 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown
threshold 64 countdown 10 time_interval 10

Success.

DES-3200-28:4#
```

show traffic control	
Purpose	Used to display current traffic control settings.
Syntax	show traffic control { <portlist> }
Description	This command is used to display the current storm traffic control configuration on the Switch.
Parameters	<portlist> – Used to specify port or list of ports for which to display traffic control settings. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display traffic control setting for ports 1 to 4:

```
DES-3200-28:4#show traffic control 1-4
Command: show traffic control 1-4

Traffic Storm Control Trap :[None]

Port Thres Broadcast Multicast Unicast Action Count Time
  hold Storm Storm Storm down Interval
-----
1 64 Disabled Disabled Disabled drop 0 5
2 64 Disabled Disabled Disabled drop 0 5
3 64 Disabled Disabled Disabled drop 0 5
4 64 Disabled Disabled Disabled drop 0 5

Total Entries : 4

DES-3200-28:4#
```

config traffic control_trap	
Purpose	Used to configure traffic control trap.
Syntax	config traffic control_trap [none storm_occurred storm_cleared both]
Description	This command is used to configure whether storm control notification will be generated or not when traffic storm events are detected by the SW traffic storm control mechanism. Note: A traffic control trap is active only when the control action is configured as "shutdown". If the control action is "drop," there will no traps issued when a storm event is detected.
Parameters	<p>none – No notification will be generated when a storm event is detected or cleared.</p> <p>storm_occurred – A notification will be generated when a storm event is detected.</p> <p>storm_cleared – A notification will be generated when a storm event is cleared.</p> <p>both – A notification will be generated both when a storm event is detected and cleared.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure traffic control for both:

```
DES-3200-28:4#config traffic control_trap both
Command: config traffic control_trap both

Success.

DES-3200-28:4#
```

QoS COMMANDS

The Switch supports 802.1p priority queuing. The Switch has four priority queues. These priority queues are numbered from 3 (Class 3) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

Priority 0 is assigned to the Switch's Q1 queue.

Priority 1 is assigned to the Switch's Q0 queue.

Priority 2 is assigned to the Switch's Q0 queue.

Priority 3 is assigned to the Switch's Q1 queue.

Priority 4 is assigned to the Switch's Q2 queue.

Priority 5 is assigned to the Switch's Q2 queue.

Priority 6 is assigned to the Switch's Q3 queue.

Priority 7 is assigned to the Switch's Q3 queue.

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the four hardware priority queues in order, beginning with the highest priority queue, 3, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

The QoS commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config bandwidth_control	[<portlist>] {rx_rate [no_limit <value 64-1024000>] tx_rate [no_limit <value 64-1024000>]} (1)
show bandwidth_control	{<portlist>}
config scheduling	<class_id 0-3> weight <value 1-55>
config scheduling_mechanism	[strict weight_fair]
show scheduling	
show scheduling_mechanism	
config 802.1p user_priority	<priority 0-7> <class_id 0-3>
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> all] <priority 0-7>
show 802.1p default_priority	<portlist>
config cos mapping ports	[<portlist> all] [none {ethernet [802.1p] ip [tos dscp]}] (1)
show cos mapping	{port <portlist> }
config cos tos value	<value 0-7> [class <class_id 0-3>]
show cos tos	{value <value 0-7>}
config dscp_mapping	dscp_value <value 0-63> [class <class_id 0-3>]
show dscp_mapping	{dscp_value <value 0-63> }

Each command is listed, in detail, in the following sections:

config bandwidth_control	
Purpose	Used to configure bandwidth control on a port by-port basis.
Syntax	config bandwidth_control [<portlist>] {rx_rate [no_limit <value 64-1024000>] tx_rate [no_limit <value 64-1024000>]} (1)
Description	This command is used to configure bandwidth on a port by-port basis.
Parameters	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p>rx_rate – Specifies that one of the parameters below (no_limit or <value 64-1024000>) will be applied to the rate at which the above specified ports will be allowed to receive packets</p> <p>no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.</p> <p><value 64-1024000> – Specifies the traffic limit, in Kbits, that the above ports will be allowed to receive.</p> <p>tx_rate – Specifies that one of the parameters below (no_limit or <value 64-1024000>) will be applied to the rate at which the above specified ports will be allowed to transmit packets.</p> <p>no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.</p> <p><value 64-1024000> – Specifies the traffic limit, in Kbits, that the above ports will be allowed to receive.</p> <p>Actual rate = rate entered/ minimum granularity * minimal granularity, for example: 62.5= 100/62.5 *62.5”</p> <p> number implies the closest smaller integer.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DES-3200-28:4#config bandwidth_control 1 rx_rate 64
Command: config bandwidth_control 1 rx_rate 64

Note: To perform precise bandwidth control, it is required to enable the
flow control to mitigate the retransmission of TCP traffic.

Success.

DES-3200-28:4#
```

show bandwidth_control	
Purpose	Used to display the bandwidth control table.
Syntax	show bandwidth_control {<portlist>}
Description	This command is used to display the current bandwidth control configuration on the Switch, on a port-by-port basis.
Parameters	<portlist> – Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display bandwidth control settings:

```
DES-3200-28:4#show bandwidth_control 1-5
Command: show bandwidth_control 1-5

Bandwidth Control Table

Port  RX Rate      TX Rate      Effective RX  Effective TX
     (Kbit/sec) (Kbit/sec)  (Kbit/sec)   (Kbit/sec)
-----
1     no_limit     no_limit     no_limit     no_limit
2     no_limit     no_limit     no_limit     no_limit
3     no_limit     no_limit     no_limit     no_limit
4     no_limit     no_limit     no_limit     no_limit
5     no_limit     no_limit     no_limit     no_limit

DES-3200-28:4#
```

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	config scheduling <class_id 0-3> weight <value 1-55>
Description	<p>The Switch contains four hardware priority queues. Incoming packets must be mapped to one of these four queues. This command is used to specify the rotation by which these four hardware priority queues are emptied.</p> <p>The Switch's default (if the config scheduling command is not used) is to empty the four hardware priority queues in order – from the highest priority queue (hardware queue 3) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.</p> <p>weight <value 1-55> – Specifies the weights for weighted COS queuing. A value between 1 and 55 can be specified.</p>
Parameters	<class_id 0-3> – This specifies which of the four hardware priority queues the config scheduling command will apply to. The four hardware priority queues are identified by number – from 0 to 3 – with the 0 queue being the lowest priority.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each queue:

```
DES-3200-28:4# config scheduling 0 weight 55
Command: config scheduling 0 weight 55

Success.

DES-3200-28:4#
```

show scheduling

Purpose	Used to display the currently configured traffic scheduling on the Switch.
Syntax	show scheduling
Description	This command is used to display the current traffic scheduling mechanisms in use on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```
DES-3200-28:4#show scheduling
Command: show scheduling

QoS Output Scheduling

Class ID      Weight
-----
Class-0       1
Class-1       2
Class-2       4
Class-3       8

DES-3200-28:4#
```

config scheduling_mechanism

Purpose	Used to configure the scheduling mechanism for the QoS function
Syntax	config scheduling_mechanism [strict weight_fair]
Description	<p>This command is used to select between a weight fair and a strict mechanism for emptying the priority classes of service of the QoS function. The Switch contains four hardware priority classes of service. Incoming packets must be mapped to one of these four hardware priority classes of service. This command is used to specify the rotation by which these four hardware priority classes of service are emptied.</p> <p>The Switch's default is to empty the four priority classes of service in order – from the highest priority class of service (queue 3) to the lowest priority class of service (queue 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority class of service to transmit its packets. Lower classes of service will be pre-empted from emptying its queue if a packet is received on a higher class of service. The packet that was received on the higher class of service will transmit its packet before allowing the lower class to resume clearing its queue.</p>
Parameters	<p>strict – Entering the strict parameter indicates that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before lower ones begin.</p> <p>weight_fair – Entering the weight fair parameter indicates that the priority classes of service will empty packets in a fair weighted order. That is to say that they will be emptied in an even distribution.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each QoS queue:


```
DES-3200-28:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DES-3200-28:4#
```

show scheduling_mechanism

Purpose	Used to display the current traffic scheduling mechanisms in use on the Switch.
Syntax	show scheduling_mechanism
Description	This command is used to display the current traffic scheduling mechanisms in use on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the scheduling mechanism:

```
DES-3200-28:4#show scheduling_mechanism
Command: show scheduling_mechanism

QOS Scheduling mechanism
CLASS ID  Mechanism
-----  -
Class-0   strict
Class-1   strict
Class-2   strict
Class-3   strict

DES-3200-28:4#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the four hardware queues available on the Switch.																											
Syntax	config 802.1p user_priority <priority 0-7> <class_id 0-3>																											
Description	<p>This command is used to configure the way the Switch will map an incoming packet, based on its 802.1p user priority, to one of the four available hardware priority queues on the Switch.</p> <p>The Switch's default is to map the following incoming 802.1p user priority values to the four hardware priority queues:</p> <table border="1"> <thead> <tr> <th>802.1p</th> <th>Hardware Queue</th> <th>Remark</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>1</td> <td>Mid-low</td> </tr> <tr> <td>1</td> <td>0</td> <td>Lowest</td> </tr> <tr> <td>2</td> <td>0</td> <td>Lowest</td> </tr> <tr> <td>3</td> <td>1</td> <td>Mid-low</td> </tr> <tr> <td>4</td> <td>2</td> <td>Mid-high</td> </tr> <tr> <td>5</td> <td>2</td> <td>Mid-high</td> </tr> <tr> <td>6</td> <td>3</td> <td>Highest</td> </tr> <tr> <td>7</td> <td>3</td> <td>Highest.</td> </tr> </tbody> </table> <p>This mapping scheme is based upon recommendations contained in IEEE 802.1D. Change this mapping by specifying the 802.1p user priority users want to map to the <class_id 0-3> (the number of the hardware queue).</p> <p><priority 0-7> – The 802.1p user priority to associate with the class_id (the number of the hardware queue).</p> <p><class_id 0-3> – The number of the Switch's hardware priority queue. The Switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).</p>	802.1p	Hardware Queue	Remark	0	1	Mid-low	1	0	Lowest	2	0	Lowest	3	1	Mid-low	4	2	Mid-high	5	2	Mid-high	6	3	Highest	7	3	Highest.
802.1p	Hardware Queue	Remark																										
0	1	Mid-low																										
1	0	Lowest																										
2	0	Lowest																										
3	1	Mid-low																										
4	2	Mid-high																										
5	2	Mid-high																										
6	3	Highest																										
7	3	Highest.																										
Restrictions	Only Administrator-level users can issue this command.																											

Example usage:

To configure 802.1p user priority on the Switch:

```
DES-3200-28:4#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-3200-28:4#
```

show 802.1p user_priority

Purpose	Used to display the current mapping between an incoming packet's 802.1p priority value and one of the Switch's four hardware priority queues.
Syntax	show 802.1p user_priority
Description	This command is used to display the current mapping of an incoming packet's 802.1p priority value to one of the Switch's four hardware priority queues.
Parameters	None.
Restrictions	None.

Example usage:

To display 802.1p user priority:

```
DES-3200-28:4#show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

Priority-0 -> <Class-1>
Priority-1 -> <Class-0>
Priority-2 -> <Class-0>
Priority-3 -> <Class-1>
Priority-4 -> <Class-2>
Priority-5 -> <Class-2>
Priority-6 -> <Class-3>
Priority-7 -> <Class-3>

DES-3200-28:4#
```

config 802.1p default_priority

Purpose	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.
Syntax	config 802.1p default_priority [<portlist> all] <priority 0-7>
Description	This command is used to specify default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine to which of the four hardware priority queues the packet is forwarded.
Parameters	<portlist> – Specifies a port or range of ports to be configured. all – Specifies that the command applies to all ports on the Switch. <priority 0-7> – The priority value to assign to untagged packets received by the Switch or a range of ports on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the Switch:

```
DES-3200-28:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3200-28:4#
```

show 802.1p default_priority

Purpose	Used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Syntax	show 802.1p default_priority {<portlist>}
Description	This command is used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Parameters	<portlist> – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the current 802.1p default priority configuration on the Switch:

```
DES-3200-28:4#show 802.1p default_priority
Command: show 802.1p default_priority
```

Port	Priority	Effective Priority
----	-----	-----
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0

```
DES-3200-28:4#
```

config cos mapping

Purpose	Used to configure the CoS to port mapping method to be used on the switch.
Syntax	config cos mapping ports [<portlist> all] [none { ethernet [802.1p] ip [tos dscp] } (1)]
Description	This command is used to set the method of which incoming packets will be identified for the CoS to port mapping feature on the Switch. Identified packets will be forwarded to the appropriate CoS queue.
Parameters	<portlist> – Specifies a port or range of ports to be configured. all – Specifies all ports will be configured. none – Disable all priority-base CoS features. ethernet – Enable Ethernet frame based priority. 802.1p – Enable 802.1p CoS ip – Enable Ethernet frame based priority.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure port 1 as CoS-enabled:

```
DES-3200-28:4#config cos mapping ports 1 ethernet 802.1p
Command: config cos mapping ports 1 ethernet 802.1p

Success.

DES-3200-28:4#
```

show cos mapping

Purpose	Used to show CoS mapping.
Syntax	show cos mapping {port <portlist> }
Description	This command is used to display information regarding CoS mapping enabled ports and their mapping method.
Parameters	<portlist> – Specifies a range of ports to be displayed. If no parameter is specified, the all ports priority settings will be shown.
Restrictions	None.

Example usage:

To show the CoS mapping information:

```
DES-3200-28:4#show cos mapping
Command: show cos mapping

Port  Ethernet_priority  IP_priority
----  -
1     802.1p              off
2     802.1p              off
3     802.1p              off
4     802.1p              off
5     802.1p              off
6     802.1p              off
7     802.1p              off
8     802.1p              off
9     802.1p              off
10    802.1p              off
11    802.1p              off
12    802.1p              off
13    802.1p              off
14    802.1p              off
15    802.1p              off
16    802.1p              off
17    802.1p              off
18    802.1p              off
19    802.1p              off
20    802.1p              off

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

config cos tos value

Purpose	Used to map the ToS value in the IP header of incoming packets to one of the four hardware queues available on the Switch.
Syntax	config cos tos value <value 0-7> [class <class_id 0-3>]
Description	This command is used to configure ToS to traffic class mapping.
Parameters	<p><value 0-7> – The ToS value of incoming packet that you want to associate with the traffic class.</p> <p><class_id 0-3> – The number of the Switch's hardware priority queue. The Switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

Configure the TOS 5 to the traffic class 1 mapping:

```
DES-3200-28:4#config cos tos value 5 class 1
Command: config cos tos value 5 class 1

Success.

DES-3200-28:4#
```

show cos tos

Purpose	Used to show TOS value to traffic class mapping.
Syntax	show cos tos {value <value 0-7>}
Description	This command is used to display the information of ToS to traffic class mappings.
Parameters	<value 0-7> – The TOS value of the incoming packet. If no parameter is specified, all the ToS values to traffic class mappings will be shown.
Restrictions	None.

Example usage:

To show the TOS to traffic class mapping of the TOS 5:

```
DES-3200-28:4#show cos tos value 5
Command: show cos tos value 5

TOS value          Class
-----
5                  2

DES-3200-28:4#
```


config dscp_mapping

Purpose	Used to map the DSCP value in the IP header of incoming packet to one of the four hardware queues available on the Switch.
Syntax	config dscp_mapping dscp_value <value 0-63> [class <class_id 0-3>]
Description	This command is used to configure DSCP mapping to traffic class.
Parameters	<p><value 0-63> – The DSCP value of the incoming packet you want to associate with the class ID.</p> <p><class_id 0-3> – The number of the Switch's hardware priority queue. The Switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DSCP map to traffic class:

```
DES-3200-28:4#config dscp_mapping dscp_value 8 class 1
Command: config dscp_mapping dscp_value 8 class 1

Success.

DES-3200-28:4#
```

show dscp_mapping

Purpose	Used to show DSCP value map to traffic class.
Syntax	show dscp_mapping {dscp_value <value 0-63>}
Description	This command displays the information for DSCP mapping to traffic class.
Parameters	<value 0-63> – The DSCP value of the incoming packet. If no parameter is specified, all the DSCP value mapping to traffic class will be shown.
Restrictions	None.

Example usage:

To show the DSCP map to traffic class:

```
DES-3200-28:4#show dscp_mapping
Command: show dscp_mapping

DSCP      Class
-----
0          0
1          0
2          0
3          0
4          0
5          0
6          0
7          0
8          0
9          0
10         0
11         0
12         0
13         0
14         0
15         0
16         0
17         0
18         0
19         0
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

PORT MIRRORING COMMANDS

The Port Mirroring commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config mirror port	<port> { [add delete] source ports <portlist> [rx tx both] }
enable mirror	
disable mirror	
show mirror	

Each command is listed, in detail, in the following sections:

config mirror port	
Purpose	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 can then be attached to study the traffic crossing the source port in a completely obtrusive manner.
Syntax	config mirror port <port> { [add delete] source ports <portlist> [rx tx both] }
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, users can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	<p><port> – This specifies the Target port (the port where mirrored packets will be received).</p> <p>[add delete] – Specifies if the user wishes to add or delete ports to be mirrored that are specified in the source ports parameter.</p> <p>source ports – The port or ports being mirrored. This cannot include the Target port.</p> <p><portlist> – This specifies a port or range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port.</p> <p>rx – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p>tx – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p>both – Mirrors all the packets received or sent by the port or ports in the port list.</p>
Restrictions	The Target port cannot be listed as a source port. Only Administrator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DES-3200-28:4#config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

DES-3200-28:4#
```

Example usage:

To delete the mirroring ports:

```
DES-3200-28:4#config mirror port 1 delete source ports 2-4 both
Command: config mirror 1 delete source ports 2-4 both

Success.

DES-3200-28:4#
```

enable mirror

Purpose	Used to enable a previously entered port mirroring configuration.
Syntax	enable mirror
Description	This command, combined with the disable mirror command below, allows the user to enter a port mirroring configuration into the Switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable mirroring configurations:

```
DES-3200-28:4#enable mirror
Command: enable mirror

Success.

DES-3200-28:4#
```

disable mirror

Purpose	Used to disable a previously entered port mirroring configuration.
Syntax	disable mirror
Description	This command, combined with the enable mirror command above, allows the user to enter a port mirroring configuration into the Switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DES-3200-28:4#disable mirror
Command: disable mirror

Success.

DES-3200-28:4#
```

show mirror

Purpose	Used to show the current port mirroring configuration on the Switch.
Syntax	show mirror
Description	This command displays the current port mirroring configuration on the Switch.
Parameters	None
Restrictions	None.

Example usage:

To display mirroring configuration:

```
DES-3200-28:4#show mirror
Command: show mirror

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

DES-3200-28:4#
```

VLAN COMMANDS

The VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
create vlan	<vlan_name 32> tag <vlanid 1-4094> {advertisement}
delete vlan	<vlan_name 32> vlanid <vidlist>
create vlan vlanid	<vidlist> {advertisement}
delete vlan vlanid	<vidlist>
config vlan vlanid	<vidlist> { [add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable] name <vlan_name 32>} (1)
config vlan	<vlan_name 32> {[add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable]} (1)
enable pvid	auto_assign
disable pvid	auto_assign
show pvid	auto_assign
config gvrp	[<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>} (1)
enable gvrp	
disable gvrp	
show vlan	{[<vlan_name 32> vlanid <vidlist> ports <portlist>]}
show gvrp	{<portlist>}

Each command is listed, in detail, in the following sections:

create vlan	
Purpose	Used to create a VLAN on the Switch.
Syntax	create vlan <vlan_name 32> tag <vlanid 1-4094> {advertisement}
Description	This command allows the user to create a VLAN on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN to be created. <vlanid 1-4094> – The VLAN ID of the VLAN to be created. Allowed values = 1-4094 advertisement – Specifies that the VLAN is able to join GVRP. If this parameter is not set, the VLAN cannot be configured to have forbidden ports.
Restrictions	Each VLAN name can be up to 32 characters. Up to 4094 static VLANs may be created per configuration. Only Administrator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DES-3200-28:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DES-3200-28:4#
```

delete vlan

Purpose	Used to delete a previously configured VLAN on the Switch.
Syntax	delete vlan <vlan_name 32> vlanid <vidlist>
Description	This command will delete a previously configured VLAN on the Switch.
Parameters	<vlan_name 32> – The VLAN name of the VLAN to delete. <vidlist> – Specifies a range of multiple VLAN IDs to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To remove the VLAN “v1”:

```
DES-3200-28:4#delete vlan v1
Command: delete vlan v1

Success.

DES-3200-28:4#
```

config vlan

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	config vlan <vlan_name 32> {[add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable]} (1)
Description	This command is used to add ports to the port list of a previously configured VLAN. The user can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	<vlan_name 32> – The name of the VLAN to which to add ports. add – Entering the add parameter will add ports to the VLAN. There are three types of ports to add: tagged – Specifies the additional ports as tagged. untagged – Specifies the additional ports as untagged. forbidden – Specifies the additional ports as forbidden delete – Deletes ports from the specified VLAN. <portlist> – A port or range of ports to add to, or delete from the specified VLAN. advertisement [enable disable] – Enables or disables GVRP on the specified VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3200-28:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DES-3200-28:4#
```

To delete ports from a VLAN:

```
DES-3200-28:4#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.

DES-3200-28:4#
```

create vlan vlanid

Purpose	Used to create multiple VLANs by VLAN ID list on the Switch.
Syntax	create vlan vlanid <vidlist> {advertisement}
Description	This command is used to create multiple VLANs on the Switch.
Parameters	<vidlist> – Specifies a range of multiple VLAN IDs to be created. advertisement – Join GVRP or not. If not, the VLAN can't join dynamically.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a VLAN ID on the Switch:

```
DES-3200-28:4#create vlan vlanid 5 advertisement
Command: create vlan vlanid 5 advertisement

Success

DES-3200-28:4#
```

delete vlan vlanid

Purpose	Used to delete multiple VLANs by VLAN ID on the Switch.
Syntax	delete vlan vlanid <vidlist>
Description	This command is used to delete previously configured multiple VLANs on the Switch.
Parameters	<vidlist> – Specifies a range of multiple VLAN IDs to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a VLAN ID on the Switch:

```
DES-3200-28:4#delete vlan vlanid 5
Command: delete vlan vlanid 5

Success

DES-3200-28:4#
```

config vlan vlanid	
Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	config vlan vlanid <vidlist> { [add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable] name <vlan_name 32>} (1)
Description	<p>This command is used to add or delete ports of the port list of previously configured VLAN(s). Specify the additional ports as being tagged, untagged or forbidden. The same port is allowed to be an untagged member port of multiple VLAN's.</p> <p>If the ports will join GVRP or not with the advertisement parameter can also be specified. The name parameter allows the name of the VLAN that needs to be modified to be specified.</p>
Parameters	<p><vidlist> – Specifies a range of multiple VLAN IDs to be configured.</p> <p>tagged – Specifies the additional ports as tagged.</p> <p>untagged – Specifies the additional ports as untagged.</p> <p>forbidden – Specifies the additional ports as forbidden.</p> <p><portlist> – A range of ports to add to the VLAN.</p> <p>advertisement – Entering the advertisement parameter specifies if the port should join GVRP or not. There are two parameters:</p> <p>enable – Specifies that the port should join GVRP.</p> <p>disable – Specifies that the port should not join GVRP.</p> <p>name – Entering the name parameter specifies the name of the VLAN to be modified.</p> <p><vlan_name 32> – Enter a name for the VLAN</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add an additional port to a previously configured VLAN on the Switch:

```
DES-3200-28:4#config vlan vlanid 5 add tagged 7 advertisement enable name
RG
Command: config vlan vlanid 5 add tagged 7 advertisement enable name RG

Success.

DES-3200-28:4#
```

enable pvid auto_assign

Purpose	Used to enable auto-assignment of PVID.
Syntax	enable pvid auto_assign
Description	This command is used to enable auto-assignment of PVID.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable auto-assignment of PVID:

```
DES-3200-28:4#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DES-3200-28:4#
```

disable pvid auto_assign

Purpose	Used to disable the auto-assignment of PVID.
Syntax	disable pvid auto_assign
Description	This command is used to disable the auto-assignment of PVID.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the auto-assignment of PVID:

```
DES-3200-28:4#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DES-3200-28:4#
```

show pvid auto_assign

Purpose	Used to display the PVID auto-assignment state.
Syntax	show pvid auto_assign
Description	This command is used to display the PVID auto-assignment state.
Parameters	None.
Restrictions	None.

Example usage:

To display the PVID auto-assignment state:

```
DES-3200-28:4#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DES-3200-28:4#
```

config gvrp	
Purpose	Used to configure GVRP on the Switch.
Syntax	config gvrp [<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>} (1)
Description	This command is used to configure the Group VLAN Registration Protocol on the Switch. Ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID) can be configured.
Parameters	<p><portlist> – A port or range of ports for which users want to enable GVRP for.</p> <p>all – Specifies all of the ports on the Switch.</p> <p>state [enable disable] – Enables or disables GVRP for the ports specified in the port list.</p> <p>ingress_checking [enable disable] – Enables or disables ingress checking for the specified port list.</p> <p>acceptable_frame [tagged_only admit_all] – This parameter states the frame type that will be accepted by the Switch for this function. tagged_only implies that only VLAN tagged frames will be accepted, while admit_all implies tagged and untagged frames will be accepted by the Switch.</p> <p>pvid <vlanid 1-4094> – Specifies the default VLAN associated with the port.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3200-28:4#config gvrp 1-4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
Command: config gvrp 1-4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Success.

DES-3200-28:4#
```

enable gvrp

Purpose	Used to enable GVRP on the Switch.
Syntax	enable gvrp
Description	This command, along with disable gvrp below, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DES-3200-28:4#enable gvrp
Command: enable gvrp

Success.

DES-3200-28:4#
```

disable gvrp

Purpose	Used to disable GVRP on the Switch.
Syntax	disable gvrp
Description	This command, along with enable gvrp, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DES-3200-28:4#disable gvrp
Command: disable gvrp

Success.

DES-3200-28:4#
```

show vlan

Purpose	Used to display the current VLAN configuration on the Switch
Syntax	show vlan [<vlan_name 32> vlanid <vidlist> ports <portlist>]
Description	This command is used to display summary information about each VLAN including the VLAN ID, VLAN name, VLAN Type, the Tagging/Untagging status, and the Member/Non-member/Forbidden status of each port that is a member of the VLAN.
Parameters	<p><vlan_name 32> – The VLAN name of the VLAN for which to display a summary of settings.</p> <p>vlanid <vidlist> – Specifies a range of multiple VLAN IDs to be displayed.</p> <p>ports <portlist> – Specifies a port or range of ports that will be</p>

show vlan

displayed.
Restrictions None.

Example usage:

To display the Switch's current VLAN settings:

```
DES-3200-28:4#show vlan
Command: show vlan
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-3200-28:4#
```

To display the Switch's current VLAN settings for a specific port:

```
DES-3200-28:4#show vlan port 1
Command: show vlan ports 1

Port 1
VLAN ID  Untagged  Tagged  Forbidden  Dynamic
-----  -
1         X         -         -         -

DES-3200-28:4#
```

show gvrp

Purpose	Used to display the GVRP status for a port list on the Switch.
Syntax	show gvrp {<portlist>}
Description	This command is used to display the GVRP status for a port list on the Switch.
Parameters	<portlist> – Specifies a port or range of ports for which the GVRP status is to be displayed.
Restrictions	None.

Example usage:

To display GVRP port status:

```

DES-3200-28:4#show gvrp 1-10
Command: show gvrp 1-10

Global GVRP : Disabled

Port  PVID  Reassigned  GVRP  Ingress  Acceptable Frame Type
      PVID                State  Checking
-----
1     1     -          Disabled  Enabled  All Frames
2     1     -          Disabled  Enabled  All Frames
3     1     -          Disabled  Enabled  All Frames
4     1     -          Disabled  Enabled  All Frames
5     1     -          Disabled  Enabled  All 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

Total Entries : 10
    
```

LINK AGGREGATION COMMANDS

The Link Aggregation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
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]} (1)
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_ports	<portlist> mode [active passive]
show lacp_ports	{<portlist>}

Each command is listed, in detail, in the following sections:

create link_aggregation	
Purpose	Used to create a link aggregation group on the Switch.
Syntax	create link_aggregation group_id <value> {type[lacp static]}
Description	This command is used to create a link aggregation group with a unique identifier.
Parameters	<p><value> – Specifies the group ID. The Switch allows up to 14 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p>type – Specify the type of link aggregation used for the group. If the type is not specified the default type is static.</p> <p>lacp – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices.</p> <p>static – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunk group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DES-3200-28:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.
DES-3200-28:4#
```

delete link_aggregation group_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	delete link_aggregation group_id <value>
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<value> – Specifies the group ID. The Switch allows up to 14 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DES-3200-28:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DES-3200-28:4#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	config link_aggregation group_id <value> {master_port <port> ports <portlist> state [enable disable]} (1)
Description	This command is used to configure a link aggregation group that was created with the create link_aggregation command above.
Parameters	group_id <value> – Specifies the group ID. The Switch allows up to 14 link aggregation groups to be configured. The group number identifies each of the groups. master_port <port> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. ports <portlist> – Specifies a port or range of ports that will belong to the link aggregation group. state [enable disable] – Allows users to enable or disable the specified link aggregation group.
Restrictions	Only Administrator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

To define a load-sharing group of ports, group-id 1, master port 1 with group members ports 1 through 4:

```
DES-3200-28:4#config link_aggregation group_id 1 master_port 1 ports 1-4
Command: config link_aggregation group_id 1 master_port 1 ports 1-4

Success.

DES-3200-28:4#
```

config link_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
----------------	---

config link_aggregation algorithm	
Syntax	config link_aggregation algorithm [mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest]
Description	This command is used to configure the part of the packet examined by the Switch when selecting the egress port for transmitting load-sharing data. This feature is only available using the address-based load-sharing algorithm.
Parameters	<p>mac_source – Indicates that the Switch should examine the MAC source address.</p> <p>mac_destination – Indicates that the Switch should examine the MAC destination address.</p> <p>mac_source_dest – Indicates that the Switch should examine the MAC source and destination addresses</p> <p>ip_source – Indicates that the Switch should examine the IP source address.</p> <p>ip_destination – Indicates that the Switch should examine the IP destination address.</p> <p>ip_source_dest – Indicates that the Switch should examine the IP source and destination addresses</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3200-28:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3200-28:4#
```

show link_aggregation	
Purpose	Used to display the current link aggregation configuration on the Switch.
Syntax	show link_aggregation {group_id <value> algorithm}
Description	This command is used to display the current link aggregation configuration of the Switch.
Parameters	<p><value> – Specifies the group ID. The Switch allows up to 14 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p>algorithm – Allows users to specify the display of link aggregation by the algorithm in use by that Switch.</p>
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DES-3200-28:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source

Group ID      : 1
Type:         : TRUNK
Master Port   :
Member Port   :
Active Port   :
Status        : Disabled
Flooding Port : 0

Total Entries : 1

DES-3200-28:4#
```

config lacp_ports

Purpose	Used to configure settings for LACP compliant ports.
Syntax	config lacp_ports <portlist> mode [active passive]
Description	This command is used to configure ports that have been previously designated as LACP ports (see create link_aggregation).
Parameters	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p>mode – Select the mode to determine if LACP ports will process LACP control frames.</p> <p>active – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.</p> <p>passive – LACP ports that are designated as passive cannot process LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have “active” LACP ports (see above).</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DES-3200-28:4#config lacp_ports 1-12 mode active
Command: config lacp_ports 1-12 mode active

Success.

DES-3200-28:4#
```

show lacp_ports

Purpose	Used to display current LACP port mode settings.
----------------	--

show lacp_ports

Syntax	show lacp_ports {<portlist>}
Description	This command is used to display the LACP mode settings as they are currently configured.
Parameters	<portlist> – Specifies a port or range of ports to be configured. If no parameter is specified, the system will display the current LACP status for all ports.
Restrictions	None.

Example usage:

To display LACP port mode settings:

```
DES-3200-28:4#show lacp_ports 1-10
Command: show lacp_ports 1-10

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

DES-3200-28:4#
```

BASIC IP COMMANDS

The Basic IP interface commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config ipif	[System] [{ ipaddress <network_address> vlan <vlan_name 32> state [enable disable] }(1) bootp dhcp dhcp_option12 [hostname <hostname 63> clear_hostname state [enable disable]] ipv6 ipv6address <ipv6networkaddr>]
show ipif	
enable autoconfig*	
disable autoconfig	

Each command is listed, in detail, in the following sections:

*See Switch Utility Commands for descriptions of all autoconfig commands.

config ipif

Purpose	Used to configure the System IP interface.
Syntax	[System] [{ ipaddress <network_address> vlan <vlan_name 32> state [enable disable] }(1) bootp dhcp dhcp_option12 [hostname <hostname 63> clear_hostname state [enable disable]] ipv6 ipv6address <ipv6networkaddr>]
Description	This command is used to configure the System IP interface on the Switch.
Parameters	<p>System – Enter System.</p> <p>ipaddress <network_address> – IP address and netmask of the IP interface to be created. Users can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format 10.1.2.3/8).</p> <p>vlan <vlan_name 32> – The name of the VLAN corresponding to the System IP interface.</p> <p>state [enable disable] – Allows users to enable or disable the IPv4 and IPv6 interface.</p> <p>bootp – Allows the selection of the BOOTP protocol for the assignment of an IPv4 IP address to the Switch's System IP interface.</p> <p>dhcp – Allows the selection of the DHCP protocol for the assignment of an IPv4 IP address to the Switch's System IP interface. If users are using the autoconfig feature, the Switch becomes a DHCP client automatically after rebooting so it is not necessary to change the ipif settings.</p> <p>ipv6 ipv6address <ipv6networkaddr> – IPV6 network address. The address should specify a host address and length of network prefix length. There can be multiple V6 addresses defined on an interface. Thus, as a new address is defined, it is added on this ipif.</p> <p>dhcp option12 hostname - Specify the host name to be inserted in the DHCP discover (DHCPDISCOVER) and DHCP request (DHCPREQUEST) message. Rules for the host name specified are as follows: The specified host name must start with a letter, end with a letter or digit. Use only letters, digits, and hyphen as interior characters. The maximum length is 63. By default, the hostname is empty.</p> <p>dhcp option12 clear_hostname - To clear the hostname setting. If the host name is empty, the system name will be used to encode option 12. If the length of system name is more than 63, superfluous characters are truncated. If the system name is also empty, the product model name is used to encode option 12.</p> <p>dhcp option12 state – Specify to enable or disable insertion of option 12 (host name) in the DHCP discover (DHCPDISCOVER) and DHCP request (DHCPREQUEST) message. By default, option 12 state is disabled.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure an interface's IPv4 network address:

```
DES-3200-28F:4# config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DES-3200-28F:4#
```

To configure an interface's DHCP option12 host name:

```
DES-3200-28F:4# config ipif System dhcp_option12 hostname switch1234
Command: config ipif System dhcp_option12 hostname switch1234

Success.

DES-3200-28F:4#
```

To configure an interface's DHCP option12 state:

```
DES-3200-28F:4# config ipif System dhcp_option12 state enable
Command: config ipif System dhcp_option12 state enable

Success.

DES-3200-28F:4#
```

show ipif

Purpose	Used to display the configuration of an IP interface on the Switch.
Syntax	show ipif
Description	This command will display the configuration of an IP interface on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display IP interface settings:

```
DES-3200-28F:4# show ipif
Command: show ipif

IP Interface Settings

Interface Name      : System
IP Address          : 192.168.1.66    (MANUAL)
Subnet Mask         : 255.0.0.0
VLAN Name           : default
Admin. State        : Enabled
Link Status         : Link UP
Member Ports        : 1-28
IPv6 Link-Local Address : FE80::208:7FF:FE06:521/128
DHCP Option12 State : Enabled
DHCP Option12 Host Name : switch123

Total              Entries
: 1

DES-3200-28F:4#
```

enable autoconfig

Purpose	Used to activate the auto configuration function for the Switch. This will load a previously saved configuration file for current use.
Syntax	enable autoconfig
Description	When autoconfig is enabled on the Switch, the DHCP reply will contain a configuration file and path name. It will then request the file from the TFTP server specified in the reply. When autoconfig is enabled, the ipif settings will automatically become DHCP client.
Parameters	None.
Restrictions	When autoconfig is enabled, the Switch becomes a DHCP client automatically (same as: config ipif System dhcp). The DHCP server must have the TFTP server IP address and configuration file name, and be configured to deliver this information in the data field of the DHCP reply packet. The TFTP server must be running and have the requested configuration file in its base directory when the request is received from the Switch. Consult the DHCP server and TFTP server software instructions for information on loading a boot file or configuration file. Only Administrator-level users can issue this command.

Example usage:

To enable auto configuration on the Switch:

```
DES-3200-28:4#enable autoconfig
Command: enable autoconfig

Success.

DES-3200-28:4#
```



NOTE: More detailed information for this command and related commands can be found in the section titled Switch Utility Commands.

disable autoconfig

Purpose	Used to disable DHCP auto configuration.
Syntax	disable autoconfig
Description	This command is used to disable the DHCP auto configuration function.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable auto configuration on the Switch:

```
DES-3200-28:4#disable autoconfig
Command: disable autoconfig

Success.

DES-3200-28:4#
```

IGMP SNOOPING COMMANDS

The IGMP Snooping commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config igmp_snooping	[vlan_name <vlan_name 32> vlanid <vidlist> all] {state [enable disable] fast_leave [enable disable]} (1)
config igmp_snooping querier	[vlan_name <vlan_name 32> vlanid <vidlist> all] {query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable] version <value 1-3>} (1)
config router_ports	[<vlan_name 32> vlanid <vidlist>] [add delete] <portlist>
config router_ports_forbidden	[<vlan_name 32> vlanid <vidlist>] [add delete] <portlist>
enable igmp_snooping	{forward_mcrouter_only}
show igmp_snooping	{vlan <vlan_name 32> } vlanid <vidlist>}
disable igmp_snooping	{forward_mcrouter_only}
show router_ports	{[vlan <vlan_name 32> vlanid <vidlist>]} {[static dynamic forbidden]}
show igmp_snooping group	{[vlan <vlan_name 32> vlanid <vidlist>]} {data_driven}
config igmp_snooping data_driven_learning	[vlan_name <vlan_name 32> vlanid <vidlist> all] {aged_out [enable disable]} (1)
config igmp_snooping data_driven_learning max_learned_entry	<value 1-1024>
clear igmp_snooping data_driven_group	[all [vlan_name <vlan_name 32> vlanid <vlanid>] [<ipaddr>] all]
show igmp_snooping host	{[vlan <vlan_name 32> vlanid <vidlist> ports <portlist> group <ipaddr>] }
config igmp access_authentication ports	[<portlist> all] state [enable disable]
show igmp access_authentication ports	[all <portlist>]

Each command is listed, in detail, in the following sections:

config igmp_snooping

Purpose	Used to configure IGMP snooping on the Switch.
Syntax	config igmp_snooping [vlan_name <vlan_name 32> vlanid <vidlist> all] {state [enable disable] fast_leave [enable disable]} (1)
Description	This command is used to configure IGMP snooping on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p><vidlist> – Specifies a list of VLANs to be configured.</p> <p>all – Specifies that all VLANs configured on the Switch will be configured.</p> <p>fast_leave [enable disable] – Enable or disable the IGMP snooping fast-leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message and the host that sends the leave message is the last host for the group.</p>

config igmp_snooping

state [enable | disable] – Allows users to enable or disable IGMP snooping for the specified VLAN.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-3200-28:4#config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

DES-3200-28:4#
```

config igmp_snooping querier

Purpose 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.

Syntax config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vidlist> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>} (1)

Description This command is used to configure the IGMP snooping querier.

Parameters <vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured.

<vidlist> – The VID range for which the IGMP snooping querier is to be configured.

all – Specifies that all VLANs configured on the Switch will be configured.

query_interval <sec 1-25> – Specifies the amount of time in seconds between general query transmissions. the default setting is 125 seconds.

max_response_time – The maximum time in seconds to wait for reports from members. The default setting is 10 seconds.

robustness_variable – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:

- Group membership interval – Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
- Other querier present interval – Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
- Last member query count – Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.
- By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy.

last_member_query_interval – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.

state – If the state is enable, it allows the switch to be selected as an IGMP

config igmp_snooping querier

Querier (sends IGMP query packets). If the state is disabled, then the switch can not play the role as a querier. Note that if the Layer 3 router connected to the switch provide only the IGMP proxy function but not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.

version – Specifies the version of IGMP packet that will be sent by this VLAN.

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To configure IGMP snooping querier:

```
DES-3200-28:4#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-3200-28:4#
```

config router_ports

Purpose	Used to configure ports as router ports.
Syntax	config router_ports [<vlan_name 32> vlanid <vidlist>] [add delete] <portlist>
Description	This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	<vlan_name 32> – The name of the VLAN on which the router port resides. <vidlist> – The VID range of the router ports to be configured. [add delete] – Specifies whether to add or delete router ports to be configured. <portlist> – Specifies a range of ports to be configured.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set up static router ports:

```
DES-3200-28:4#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DES-3200-28:4#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden router ports.
Syntax	config router_ports_forbidden [<vlan_name 32> vlanid <vidlist>] [add delete] <portlist>

config router_ports_forbidden

Description	This command is used to allow designation of a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p><vidlist> – The VID range of the ports to be configured as forbidden ports.</p> <p>[add delete] – Specifies whether to add or delete forbidden ports of the specified VLAN.</p> <p><portlist> – Specifies a range of ports that will be configured as forbidden router ports.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set up forbidden router ports:

```
DES-3200-28:4#config router_ports_forbidden default add 2-10
Command: config router_ports_forbidden default add 2-10

Success.

DES-3200-28:4#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	enable igmp_snooping {forward_mcrouter_only}
Description	This command is used to enable IGMP snooping on the Switch. If forward_mcrouter_only is specified, the Switch will learn the router port based on identification of the multicast routing protocol packet and the IGMP control packet.
Parameters	forward_mcrouter_only – Adding this parameter to the command, the Switch will learn the router port based on identification of the multicast routing protocol packet and the IGMP control packet.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DES-3200-28:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3200-28:4#
```

disable igmp_snooping	
Purpose	Used to disable IGMP snooping on the Switch.
Syntax	disable igmp_snooping {forward_mcrouter_only}
Description	This command is used to disable IGMP snooping on the Switch. If forward_mcrouter_only is specified, the Switch will learn the router port based on identification of the unicast routing protocol packet, the multicast routing protocol packet, and the IGMP control packet. For command backward compatibility, this command will be supported in the CLI, but it does not effect the system behavior of router port learning.
Parameters	forward_mcrouter_only – Adding this parameter to this command, the Switch will learn the router port based on identification of the unicast routing protocol packet, the multicast routing protocol packet, and the IGMP control packet, and the disable igmp_snooping forward_mcrouter_only command will not take effect. The Switch will learn the router port based on identification of the multicast routing protocol packet and the IGMP control packet.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DES-3200-28:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3200-28:4#
```

show igmp_snooping	
Purpose	Used to show the current status of IGMP snooping on the Switch.
Syntax	show igmp_snooping {vlan <vlan_name 32> vlanid <vidlist>}
Description	This command is used to display the current IGMP snooping status and configuration on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN for which to view the IGMP snooping configuration. <vidlist> – The VID range of the configuration to be displayed.
Restrictions	None.

Example usage:

To show IGMP snooping:

```
DES-3200-28:4#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State      : Disabled
Multicast Router Only           : Disabled
Data Driven Learning Max Entries : 56

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
Version                         : 3
Data Driven Learning Aged Out   : Disabled

Total Entries : 1

DES-3200-28:4#
```

show router_ports	
Purpose	Used to display the currently configured router ports on the Switch.
Syntax	show router_ports {[vlan <vlan_name 32> vlanid <vidlist>]} {[static dynamic forbidden]}
Description	This command is used to display the router ports currently configured on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN on which the router port resides. <vidlist> – The VID range of the router ports to be displayed. static – Displays router ports that have been statically configured. dynamic – Displays router ports that have been dynamically configured. forbidden – Displays forbidden router ports that have been statically configured.
Restrictions	None.

Example usage:

To display the router ports.

```
DES-3200-28:4#show router_ports
Command: show router_ports

VLAN Name      : default
Static Router Port :
Dynamic Router Port:
Forbidden Router Port:

Total Entries: 1

DES-3200-28:4#
```

show igmp_snooping group	
Purpose	Used to display the current IGMP snooping group configuration on the Switch.
Syntax	show igmp_snooping group {[vlan <vlan_name 32> vlanid <vidlist>]} {data_driven}
Description	This command will display the current IGMP snooping group configuration on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN for which to view IGMP snooping group information. <vidlist> – The VID list for which to view IGMP snooping group information. data_driven – Display the data driven groups.
Restrictions	None.

Example usage:

To view the current IGMP snooping group:

```
DES-3200-28:4#show igmp_snooping group
Command: show igmp_snooping group

Source/Group    : NULL/239.255.255.255
VLAN Name/VID   : default/1
Reports         : 1
Member Ports    : 4
Router Ports    : 8
Up time         : 122
Expire Time     : 260
Filter Mode     : EXCLUDE

Total Entries   : 1

DES-3200-28:4#
```


config igmp_snooping data_driven_learning

Purpose	Used to configure the data driven learning of an IGMP snooping group.
Syntax	config igmp_snooping data_driven_learning [vlan_name <vlan_name> vlanid <vidlist> all] { aged_out [enable disable]} (1)
Description	This command is used to enable or disable the age-out of data driven learning of an IGMP snooping group.
Parameters	<p><vlan_name 32> – Specifies the VLAN name to be configured.</p> <p><vidlist> – Specifies the VID range to be configured.</p> <p>all – Specifies that all VLANs configured on the Switch will be configured.</p> <p>aged_out – Used to enable/disable the aging on the entry. By default, the state is in disabled state.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the IGMP snooping data driven entry:

```
DES-3200-28:4#config igmp_snooping data_driven_learning vlan_name default
aged_out enable
Command: config igmp_snooping data_driven_learning vlan_name default
aged_out enable

Success.

DES-3200-28:4#
```

config igmp_snooping data_driven_learning max_learned_entry

Purpose	Used to configure the maximum number of groups that can be learned by data driven.
Syntax	config igmp_snooping data_driven_learning max_learned_entry <value 1-1024>
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 learning new data-driven groups.
Parameters	<value 1-1024> - The maximum number of groups that can be learned by data driven. The default value is 56.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure IGMP snooping data driven learning's maximum learned entry value:

```
DES-3200-28:4# config igmp_snooping data_driven_learning max_learned_entry
1
Command: config igmp_snooping data_driven_learning max_learned_entry 1

Success.

DES-3200-28:4#
```

clear igmp_snooping data_driven_group

Purpose	Used to delete the IGMP snooping group learned by data driven.
Syntax	clear igmp_snooping data_driven_group [[vlan_name <vlan_name 32> vlanid <vlanid>] [all <ipaddress>] all]
Description	This command is used to delete the IGMP snooping group learned by data driven. Note that this command is currently only for layer 2 switches.
Parameters	<vlan_name 32> – Specifies the VLAN name. <vlanid> – Specifies the VLAN ID. all – Delete all data-driven entries. <ipaddr> – Specifies the IP Address. all – Delete all IP addresses.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete all the groups learned by data-driven :

```
DES-3200-28:4# clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.

DES-3200-28:4#
```

show igmp_snooping host

Purpose	Used to display the IGMP host that has joined groups on specific ports or specific VLANs.
Syntax	show igmp_snooping host {[vlan_name <vlan_name 32> vlanid <vlanid> ports <portlist> group <ipaddr>] }
Description	This command is used to display the IGMP host that has joined groups on specific ports or specific VLANs.
Parameters	<vlan_name 32> – Specifies the VLAN to display the host information. If a VLAN or port is not specified, all joining hosts will be displayed. <vlanid>– Specifies the VLAN ID. <portlist>– Specifies the list of ports to display the host information. If a VLAN or port is not specified, all joining hosts will be displayed. <ipaddr> – Specifies the IP address of a group to display the host information.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display IGMP snooping fast leave hosts:

```
DES-3200-28:4# show igmp_snooping host
Command: show igmp_snooping host

VLAN ID      Group                Port No      IGMP Host
-----      -
1            225.0.1.0           2            198.19.1.2
1            225.0.1.0           2            198.19.1.3
1            225.0.1.0           3            198.19.1.4
1            225.0.1.2           2            198.19.1.3
1            225.0.2.3           3            198.19.1.4
1            225.0.3.4           3            198.19.1.5
1            225.0.4.5           5            198.19.1.6
1            225.0.5.6           5            198.19.1.7
1            225.0.6.7           4            198.19.1.8
1            225.0.7.8           4            198.19.1.9
1            239.255.255.250    7            10.90.90.90

Total Entries : 11

DES-3200-28:4#
```

config igmp access_authentication ports	
Purpose	Used to configure the IGMP Access Control port status.
Syntax	config igmp access_authentication ports [<portlist> all] state [enable disable]
Description	This command is used to enable or disable IGMP Access Control function for specified port. When the access_authentication is enabled, and the switch received an IGMP JOIN, the switch will send the access request to the RADIUS server to do the authentication.
Parameters	<portlist> – Specifies a range of ports to be configured. state – Enable or disable the RADIUS authentication function on the specified ports.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable IGMP Access Control for all ports:

```
DES-3200-28:4# config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable

Success.

DES-3200-28:4#
```

show igmp access_authentication ports

Purpose	Used to display the current IGMP Access Control configuration.
Syntax	show igmp access_authentication ports [all <portlist>]
Description	This command is used to display the current IGMP Access Control configuration.
Parameters	<portlist> – specifies a range of ports to be displayed.
Restrictions	None.

Example usage:

To display IGMP Access Control status for ports 1 to 4:

```
DES-3200-28:4# show igmp access_authentication ports 1-4
Command: show igmp access_authentication ports 1-4

Port   Authentication State
-----
1      Enabled
2      Disabled
3      Disabled
4      Enabled

DES-3200-28:4#
```

DHCP RELAY COMMANDS

The DHCP Relay commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config dhcp_relay	{hops <value 1-16> time <sec 0-65535>} (1)
config dhcp_relay add ipif	[System] <ipaddr>
config dhcp_relay delete ipif	[System] <ipaddr>
config dhcp_relay option_82 state	[enable disable]
config dhcp_relay option_82 check	[enable disable]
config dhcp_relay option_82 policy	[replace drop keep]
config dhcp_relay option_82 remote_id	[default user_define <string 32>]
show dhcp_relay	{ipif [System]}
enable dhcp_relay	
disable dhcp_relay	

Each command is listed in detail in the following sections:

config dhcp_relay

Purpose	Used to configure the DHCP/BOOTP relay feature of the switch.
Syntax	config dhcp_relay {hops <value 1-16> time <sec 0-65535>} (1)
Description	This command is used to configure the DHCP/BOOTP relay feature.
Parameters	hops <value 1-16> – Specifies the maximum number of relay agent hops that the DHCP packets can cross. time <sec 0-65535> – If this time is exceeded; the Switch will not relay the DHCP packet.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config DHCP relay:

```
DES-3200-28:4#config dhcp_relay hops 2 time 23
Command: config dhcp_relay hops 2 time 23

Success.

DES-3200-28:4#
```

config dhcp_relay add ipif

Purpose	Used to add an IP destination address to the switch's DHCP/BOOTP relay table.
Syntax	config dhcp_relay add ipif [System] <ipaddr>
Description	This command is used to add an IP address as a destination to forward (relay) DHCP/BOOTP relay packets to.
Parameters	[System] – The name of the IP interface in which DHCP relay is to be enabled. <ipaddr> – The DHCP server IP address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add an IP destination to the DHCP relay table:

```
DES-3200-28:4#config dhcp_relay add ipif System 10.58.44.6
Command: config dhcp_relay add ipif System 10.58.44.6

Success.

DES-3200-28:4#
```

config dhcp_relay delete ipif

Purpose	Used to delete one or all IP destination addresses from the Switch's DHCP/BOOTP relay table.
Syntax	config dhcp_relay delete ipif [System] <ipaddr>
Description	This command is used to delete an IP destination addresses in the Switch's DHCP/BOOTP relay table.
Parameters	[System] – The name of the IP interface that contains the IP address below. <ipaddr> – The DHCP server IP address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an IP destination from the DHCP relay table:

```
DES-3200-28:4#config dhcp_relay delete ipif System 10.58.44.6
Command: config dhcp_relay delete ipif System 10.58.44.6

Success.

DES-3200-28:4#
```

config dhcp_relay option_82 state

Purpose	Used to configure the state of DHCP relay agent information option 82 of the Switch.
Syntax	config dhcp_relay option_82 state [enable disable]
Description	This command is used to configure the state of DHCP relay agent information option 82 of the Switch.
Parameters	<p>enable – When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP server and client. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.</p> <p>disable – If the field is toggled to disable the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DES-3200-28:4#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DES-3200-28:4#
```

config dhcp_relay option_82 check

Purpose	Used to configure the checking mechanism of DHCP relay agent information option 82 of the Switch.
Syntax	config dhcp_relay option_82 check [enable disable]
Description	This command is used to configure the checking mechanism of DHCP/BOOTP relay agent information option 82 of the Switch.
Parameters	<p>enable – When the field is toggled to enable, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option 82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages.</p> <p>disable – When the field is toggled to disable, the relay agent will not check the validity of the packet's option 82 field.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 check:

```
DES-3200-28:4#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DES-3200-28:4#
```

config dhcp_relay option_82 policy	
Purpose	Used to configure the re-forwarding policy of the relay agent information option 82 of the Switch.
Syntax	config dhcp_relay option_82 policy [replace drop keep]
Description	This command is used to configure the re-forwarding policy of DHCP relay agent information option 82 of the Switch.
Parameters	replace – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. drop – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. keep – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 policy:

```
DES-3200-28:4#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DES-3200-28:4#
```


config dhcp_relay option_82 remote id

Purpose	Used to configure the processing of the DHCP 82 remote ID option for the DHCP relay function.															
Syntax	config dhcp_relay option_82 remote_id [default user_define <string 32>]															
Description	<p>This command is used to configure the processing of the DHCP 82 option for the DHCP relay function.</p> <p>When DHCP 82 option is enabled, the DHCP packet received from the client will be inserted with the option 82 field before being relayed to the server. The DHCP 82 option contains 2 suboptions, which are circuit ID suboption and remote ID suboption.</p> <p>The formats for the circuit ID suboption and the remote ID suboption are as follows. For the circuit ID suboption of a standalone switch, the module field is always zero.</p> <p>Remote ID suboption format 2 (Using user-defined string as remote ID):</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">A.</td> <td style="text-align: center;">B.</td> <td style="text-align: center;">C.</td> <td style="text-align: center;">D.</td> <td style="text-align: center;">E.</td> </tr> <tr> <td style="text-align: center;">2</td> <td style="text-align: center;">n + 2</td> <td style="text-align: center;">1</td> <td style="text-align: center;">n</td> <td style="text-align: center;">User-defined string</td> </tr> <tr> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">6 bytes</td> </tr> </table> <p>A. Suboption type B. Length: the string length of the Remote ID suboption C. Remote ID type D. Length: the string length of a user-defined string E. User-defined string</p>	A.	B.	C.	D.	E.	2	n + 2	1	n	User-defined string	1 byte	1 byte	1 byte	1 byte	6 bytes
A.	B.	C.	D.	E.												
2	n + 2	1	n	User-defined string												
1 byte	1 byte	1 byte	1 byte	6 bytes												
Parameters	None.															
Restrictions	Only Administrator-level users can issue this command.															

Example usage:

To configure DHCP relay option 82 remote id :

```
DES-3200-28:4#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"

DES-3200-28:4#
```

show dhcp_relay

Purpose	Used to display the current DHCP/BOOTP relay configuration.
Syntax	show dhcp_relay {ipif [System]}
Description	This command is used to display the current DHCP relay configuration for the Switch.
Parameters	ipif System – The name of the IP interface for which to display the current DHCP relay configuration.
Restrictions	None.

Example usage:

To show the DHCP relay configuration:

```
DES-3200-28:4#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 Relay Agent Information Option 82 State      : Disabled
DHCP Relay Agent Information Option 82 Check      : Disabled
DHCP Relay Agent Information Option 82 Policy     : Replace
DHCP Relay Agent Information Option 82 Remote ID  : 00-19-5B-EF-78-B5

Interface      Server 1      Server 2      Server 3      Server 4
-----
DES-3200-28:4#
```

To show a single IP destination of the DHCP relay configuration:

```
DES-3200-28:4#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

Interface      Server 1      Server 2      Server 3      Server 4
-----
System         10.58.44.6

DES-3200-28:4#
```

enable dhcp_relay	
Purpose	Used to enable the DHCP/BOOTP relay function on the Switch.
Syntax	enable dhcp_relay
Description	This command is used to enable the DHCP/BOOTP relay function on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable DHCP relay:

```
DES-3200-28:4#enable dhcp_relay
Command: enable dhcp_relay

Success.

DES-3200-28:4#
```

disable dhcp_relay	
Purpose	Used to disable the DHCP/BOOTP relay function on the Switch.
Syntax	disable dhcp_relay
Description	This command is used to disable the DHCP/BOOTP relay function on the Switch.

disable dhcp_relay

Parameters None.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To disable DHCP relay:

```
DES-3200-28:4#disable dhcp_relay
```

```
Command: disable dhcp_relay
```

```
Success.
```

```
DES-3200-28:4#
```

802.1X COMMANDS

The Switch implements IEEE 802.1X Port-based and Host-based Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames. The 802.1X commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

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

Command	Parameters
show 802.1x user	

Each command is listed, in detail, in the following sections:

enable 802.1x

Purpose	Used to enable the 802.1X server on the Switch.
Syntax	enable 802.1x
Description	This command is used to enable the 802.1X Network Access control application on the Switch. To select between port-based or Host-based, use the config 802.1x auth_mode command.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable 802.1X switch wide:

```
DES-3200-28:4#enable 802.1x
Command: enable 802.1x

Success.

DES-3200-28:4#
```

disable 802.1x

Purpose	Used to disable the 802.1X server on the Switch.
Syntax	disable 802.1x
Description	This command is used to disable the 802.1X Network Access control application on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable 802.1x on the Switch:

```
DES-3200-28:4#disable 802.1x
Command: disable 802.1x

Success.

DES-3200-28:4#
```

show 802.1x

Purpose	Used to display the current authentication state and authentication configuration of the 802.1X server on the Switch.
Syntax	show 802.1x [auth_state auth_configuration] {ports <portlist>}
Description	This command is used to display the current configuration or authentication state of the 802.1X server on the Switch.

show 802.1x

Parameters	<p>auth_state – Displays the current authentication state of the 802.1X server.</p> <p>auth_configuration – Displays the current authentication configuration of the 802.1X server.</p> <p>ports <portlist> – Specifies a port or range of ports to view.</p> <p>The following details are displayed for the authentication configuration:</p> <p>802.1x Enabled / Disabled – Shows the current status of 802.1X functions on the Switch.</p> <p>Authentication Mode – Shows the authentication mode, whether it be by MAC address or by port.</p> <p>Authentication Protocol – Shows the authentication protocol suite in use between the Switch and a RADIUS server. May read Radius_Eap or local.</p> <p>Port number – Shows the physical port number on the Switch.</p> <p>Capability: Authenticator/None – Shows the capability of 802.1X functions on the port number displayed above. There are two 802.1X capabilities that can be set on the Switch: Authenticator and None.</p> <p>AdminCtlDir: Both / In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.</p> <p>OpenCtlDir: Both / In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.</p> <p>Port Control: ForceAuth / ForceUnauth / Auto – Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized.</p> <p>QuietPeriod – This is the initialization value of the quiet period timer. The default value is 60s and can be any value between 0-65535.</p> <p>TxPeriod – This us the initialization value of the tx timer. The default value is 30s and can be any value between 1-65535.</p> <p>SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request / Identity packets.</p> <p>ServerTimeout – Shows the length of time to wait for a response from a RADIUS server.</p> <p>MaxReq – Shows the maximum number of times to retry sending packets to the supplicant.</p> <p>ReAuthPeriod – Shows the time interval between successive re-authentications.</p> <p>ReAuthenticate: Enabled / Disabled – Shows whether or not to re-authenticate.</p> <p>The following details are displayed for the current authentication state:</p> <p>Port number – Shows the physical port number on the Switch.</p> <p>Auth PAE State: Initalize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE.</p> <p>Backend State: Request / Response / Fail / Idle / Initalize / Success / Timeout – Shows the current state of the Backend Authenticator.</p> <p>Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network</p>
Restrictions	None.

Example usage:

To display the 802.1X authentication states:

```
DES-3200-28:4#show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X                : Enabled
Authentication Mode   : Port_based
Authentication Protocol : Radius_EAP

Port Number          : 1
Capability           : None
AdminCrldir         : Both
OpenCrldir          : Both
Port Control         : Auto
QuietPeriod          : 60    sec
TxPeriod             : 30    sec
SuppTimeout          : 30    sec
ServerTimeout        : 30    sec
MaxReq               : 2     times
ReAuthPeriod         : 3600  sec
ReAuthenticate       : Disabled

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

To display the 802.1X authentication state for port-based 802.1X:

```
DES-3200-28:4#show 802.1x auth_state
Command: show 802.1x auth_state

Port      Auth PAE State  Backend State  Port Status
-----
1         ForceAuth      Success        Authorized
2         ForceAuth      Success        Authorized
3         ForceAuth      Success        Authorized
4         ForceAuth      Success        Authorized
5         ForceAuth      Success        Authorized
6         ForceAuth      Success        Authorized
7         ForceAuth      Success        Authorized
8         ForceAuth      Success        Authorized
9         ForceAuth      Success        Authorized
10        ForceAuth      Success        Authorized
11        ForceAuth      Success        Authorized
12        ForceAuth      Success        Authorized
13        ForceAuth      Success        Authorized
14        ForceAuth      Success        Authorized
15        ForceAuth      Success        Authorized
16        ForceAuth      Success        Authorized
17        ForceAuth      Success        Authorized
18        ForceAuth      Success        Authorized
19        ForceAuth      Success        Authorized
20        ForceAuth      Success        Authorized
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```


Example usage:

To display the 802.1X authentication state for host-based 802.1X:

```
DES-3200-28:4#show 802.1x auth_state
Command: show 802.1x auth_state

Port Number : 1
Index  MAC Address          Auth PAE State  Backend State  Port Status
-----  -----
1      00-80-C8-4D-4E-0A    Connecting     Idle           Unauthorized
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

config 802.1x auth_mode	
Purpose	Used to configure the 802.1X authentication mode on the Switch.
Syntax	config 802.1x auth_mode [port_based mac_based]
Description	This command is used to enable either the port-based or Host-based 802.1X authentication feature on the Switch.
Parameters	[port_based mac_based] – The Switch allows users to authenticate 802.1X by either port or MAC address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure 802.1X authentication by MAC address:

```
DES-3200-28:4#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DES-3200-28:4#
```

config 802.1x capability ports	
Purpose	Used to configure the 802.1X capability of a range of ports on the Switch.

config 802.1x capability ports

Syntax	config 802.1x capability ports [<portlist> all] [authenticator none]
Description	This command has two capabilities that can be set for each port, authenticator and none.
Parameters	<portlist> – Specifies a port or range of ports to be configured. all – Specifies all of the ports on the Switch. authenticator – A user must pass the authentication process to gain access to the network. none – The port is not controlled by the 802.1X functions.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure 802.1X capability on ports 1 to 10:

```
DES-3200-28:4#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DES-3200-28:4#
```

config 802.1x auth_parameter ports

Purpose	Used to configure the 802.1X Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1X settings.
Syntax	config 802.1x auth_parameter ports [<portlist> all] [default {direction [both in] port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth [enable disable]]] (1)
Description	This command is used to configure the 802.1X Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1X settings.
Parameters	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p>all – Specifies all of the ports on the Switch.</p> <p>default – Returns all of the ports in the specified range to their 802.1X default settings.</p> <p>direction [both in] – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.</p> <p>port_control – Configures the administrative control over the authentication process for the range of ports. The user has the following authentication options:</p> <p>force_auth – Forces the Authenticator for the port to become authorized. Network access is allowed.</p> <p>auto – Allows the port's status to reflect the outcome of the authentication process.</p> <p>force_unauth – Forces the Authenticator for the port to become unauthorized. Network access will be blocked.</p> <p>quiet_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authentication attempt.</p> <p>tx_period <sec 1-65535> – Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.</p> <p>supp_timeout <sec 1-65535> – Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.</p> <p>server_timeout <sec 1-65535> – Configure the length of time to wait for a response from a RADIUS server.</p> <p>max_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user).</p> <p>reauth_period <sec 1-65535> – Configures the time interval between successive re-authentications.</p> <p>enable_reauth [enable disable] – Determines whether or not the Switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure 802.1X authentication parameters for ports 1 to 20:

```
DES-3200-28:4#config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

DES-3200-28:4#
```

config 802.1x auth_protocol	
Purpose	Used to configure the 802.1X authentication protocol on the Switch.
Syntax	config 802.1x auth_protocol [local radius_eap]
Description	This command is used to configure the authentication protocol.
Parameters	local radius_eap – Specify the type of authentication protocol desired.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the authentication protocol on the Switch:

```
DES-3200-28:4# config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DES-3200-28:4#
```

config 802.1x init	
Purpose	Used to initialize the 802.1X function on a range of ports.
Syntax	config 802.1x init [port_based ports [<portlist> all] mac_based ports [<portlist> all] {mac_address <macaddr>}]
Description	This command is used to immediately initialize the 802.1X functions on a specified range of ports or for specified MAC addresses operating from a specified range of ports.
Parameters	<p>port_based – This instructs the Switch to initialize 802.1X functions based only on the port number. Ports approved for initialization can then be specified.</p> <p>mac_based – This instructs the Switch to initialize 802.1X functions based only on the port number or the MAC address. MAC addresses approved for initialization can then be specified.</p> <p>ports <portlist> – Specifies a port or range of ports to be configured.</p> <p>all – Specifies all of the ports on the Switch.</p> <p>mac_address <macaddr> – Enter the MAC address to be initialized.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To initialize the authentication state machine of all ports:

```
DES-3200-28:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-3200-28:4#
```

config 802.1x reauth

Purpose	Used to configure the 802.1X re-authentication feature of the Switch.
Syntax	config 802.1x reauth [port_based ports [<portlist> all] mac_based ports [<portlist> all] {mac_address <macaddr>}]
Description	This command is used to re-authenticate a previously authenticated device based on port number.
Parameters	<p>port_based – This instructs the Switch to re-authorize 802.1X functions based only on the port number. Ports approved for re-authorization can then be specified.</p> <p>mac_based – This instructs the Switch to re-authorize 802.1X functions based only on the port number or the MAC address. MAC addresses approved for re-authorization can then be specified.</p> <p>ports <portlist> – Specifies a port or range of ports to be re-authorized.</p> <p>all – Specifies all of the ports on the Switch.</p> <p>mac_address <macaddr> – Enter the MAC address to be re-authorized.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure 802.1X reauthentication for ports 1 to 18:

```
DES-3200-28:4#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-3200-28:4#
```

config radius add

Purpose	Used to configure the settings the Switch will use to communicate with a RADIUS server.
Syntax	config radius add <server_index 1-3> [<server_ip>] key <passwd 32> [default {auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535> timeout <int 1-255> retransmit <int 1-255>} (1)]
Description	This command is used to configure the settings the Switch will use to communicate with a RADIUS server.
Parameters	<p><server_index 1-3> – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch.</p> <p><server_ip> – The IP address of the RADIUS server.</p> <p>key – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.</p> <p><passwd 32> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used.</p> <p>default – Uses the default UDP port number in both the “auth_port” and “acct_port” settings.</p> <p>auth_port <udp_port_number 1-65535> – The UDP port number for authentication requests. The default is 1812.</p> <p>acct_port <udp_port_number 1-65535> – The UDP port number for accounting requests. The default is 1813.</p> <p>timeout <int 1-255> – The time in second for waiting server reply. The default value is 5 seconds.</p> <p>retransmit <int 1-255> – The count for re-transmit. The default value is 2.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DES-3200-28:4#config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DES-3200-28:4#
```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.
Syntax	config radius delete <server_index 1-3>
Description	This command is used to delete a previously entered RADIUS server configuration.
Parameters	<server_index 1-3> – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DES-3200-28:4#config radius delete 1
Command: config radius delete 1

Success.

DES-3200-28:4#
```

config radius

Purpose	Used to configure the Switch's RADIUS settings.
Syntax	config radius <server_index 1-3> {ipaddress <server_ip> key <passwd 32> [auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>] timeout <int 1-255> retransmit <int 1-255>} (1)
Description	This command is used to configure the Switch's RADIUS settings.
Parameters	<p><server_index 1-3> – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch.</p> <p>ipaddress <server_ip> – The IP address of the RADIUS server.</p> <p>key – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.</p> <p><passwd 32> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used.</p> <p>auth_port <udp_port_number 1-65535> – The UDP port number for authentication requests. The default is 1812.</p> <p>acct_port <udp_port_number 1-65535> – The UDP port number for accounting requests. The default is 1813.</p> <p>timeout <int 1-255> – The time in second for waiting server reply. The default value is 5 seconds.</p> <p>retransmit <int 1-255> – The count for re-transmit. The default value is 2.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DES-3200-28:4#config radius 1 10.48.74.121 key dlink default
Command: config radius 1 10.48.74.121 key dlink default

Success.

DES-3200-28:4#
```

config radius parameter	
Purpose	Used to configure parameters for RADIUS servers.
Syntax	config radius parameter {timeout <int 1-255> retransmit <int 1-255>} (1)
Description	This command is used to configure parameters for RADIUS servers.
Parameters	timeout <int 1-255> – The time in second for waiting server reply. The default value is 5 seconds. retransmit <int 1-255> – The count for re-transmit. The default value is 2.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the timeout option for RADIUS servers:

```
DES-3200-28:4# config radius parameter timeout 3
Command: config radius parameter timeout 3

Success.

DES-3200-28:4#
```

show radius	
Purpose	Used to display the current RADIUS configurations on the Switch.
Syntax	show radius
Description	This command is used to display the current RADIUS configurations on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display RADIUS settings on the Switch:

```
DES-3200-28:4#show radius
Command: show radius

Timeout      : 5 seconds
Retransmit   : 2

Index  IP Address          Auth-Port  Acct-Port  Status      Key
-----  -----
1      10.1.1.1             1812      1813      Active      switch
2      20.1.1.1             1800      1813      Active      des3200
3      30.1.1.1             1812      1813      Active      dlink

Total Entries : 3

DES-3200-28:4#
```

create 802.1x guest_vlan	
Purpose	Used to configure a pre-existing VLAN as a 802.1X Guest VLAN.
Syntax	create 802.1x guest_vlan {<vlan_name 32>}
Description	This command is used to configure a pre-defined VLAN as a 802.1X Guest VLAN. Guest 802.1X VLAN clients are those who have not been authorized for 802.1X or they haven't yet installed the necessary 802.1X software, yet would still like to have limited access rights on the Switch.
Parameters	<vlan_name 32> – Enter an alphanumeric string of no more than 32 characters to define a pre-existing VLAN as a 802.1X Guest VLAN. This VLAN must have first been created with the create vlan command mentioned earlier in this manual.
Restrictions	Only Administrator-level users can issue this command. Users must have already previously created a VLAN using the create vlan command. Only one VLAN can be set as the 802.1X Guest VLAN.

Example usage:

To configure a previously created VLAN as an 802.1X Guest VLAN for the Switch:

```
DES-3200-28:4#create 802.1x guest_vlan Tiberius
Command: create 802.1x guest_vlan Tiberius

Success.

DES-3200-28:4#
```

config 802.1x guest_vlan ports	
Purpose	Used to configure ports for a pre-existing 802.1X guest VLAN.
Syntax	config 802.1x guest_vlan ports [<portlist> all] state [enable disable]

config 802.1x guest_vlan ports

Description	This command is used to configure ports to be enabled or disabled for the 802.1X guest VLAN.
Parameters	<p><portlist> – Specify a port or range of ports to be configured for the 802.1X Guest VLAN.</p> <p>all – Specify this parameter to configure all ports for the 802.1X Guest VLAN.</p> <p>state [enable disable] – Use these parameters to enable or disable port listed here as enabled or disabled for the 802.1X Guest VLAN.</p>
Restrictions	<p>Only Administrator-level users can issue this command.</p> <p>Users must have already previously created a VLAN using the create vlan command. If the specific port state changes from an enabled state to a disabled state, these ports will return to the default VLAN.</p>

Example usage:

To configure the ports for a previously created 802.1X Guest VLAN as enabled.

```
DES-3200-28:4#config 802.1x guest_vlan ports 1-5 state enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DES-3200-28:4#
```

show 802.1x guest_vlan

Purpose	Used to view the configurations for a 802.1X Guest VLAN.
Syntax	show 802.1x guest_vlan
Description	This command is used to display the settings for the VLAN that has been enabled as an 802.1X Guest VLAN. Guest 802.1X VLAN clients are those who have not been authorized for 802.1X or they haven't yet installed the necessary 802.1X software, yet would still like to have limited access rights on the Switch.
Parameters	None.
Restrictions	<p>None.</p> <p>This VLAN is only supported for port-based 802.1X and must have already been previously created using the create vlan command. Only one VLAN can be set as the 802.1X Guest VLAN.</p>

Example usage:

To configure the configurations for a previously created 802.1X Guest VLAN:

```
DES-3200-28:4#show 802.1x guest_vlan
Command: show 802.1x guest_vlan
```

Guest VLAN Settings

```
-----
Guest VLAN : Tiberius
Enable Guest VLAN Ports: 1-5
```

```
DES-3200-28:4#
```

delete 802.1x guest_vlan

Purpose	Used to delete a 802.1X Guest VLAN.
Syntax	delete 802.1x guest_vlan {<vlan_name 32>}
Description	This command is used to delete an 802.1X Guest VLAN. Guest 802.1X VLAN clients are those who have not been authorized for 802.1X or they haven't yet installed the necessary 802.1X software, yet would still like to have limited access rights on the Switch.
Parameters	<vlan_name 32> – Enter the VLAN name of the Guest 802.1X VLAN to be deleted.
Restrictions	Only Administrator-level users can issue this command. Users must have already previously created a VLAN using the create vlan command. Only one VLAN can be set as the 802.1X Guest VLAN.

Example usage:

To delete a previously created 802.1X Guest VLAN.

```
DES-3200-28:4#delete 802.1x guest_vlan Tiberius
Command: delete 802.1x guest_vlan Tiberius
```

Success.

```
DES-3200-28:4#
```

show acct_client

Purpose	Used to display the current RADIUS accounting client.
Syntax	show acct_client
Description	This command is used to display the current RADIUS accounting client currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS accounting client:

```
DES-3200-28:4#show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses    0
radiusAcctClientIdentifier                 D-Link

radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                    10.53.13.199
radiusAccClientServerPortNumber          1813
radiusAccClientRoundTripTime              0
radiusAccClientRequests                   0
radiusAccClientRetransmissions            0
radiusAccClientResponses                  0
radiusAccClientMalformedResponses         0
radiusAccClientBadAuthenticators          0
radiusAccClientPendingRequests            0
radiusAccClientTimeouts                   0
radiusAccClientUnknownTypes               0
radiusAccClientPacketsDropped             0
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

show auth_client

Purpose	Used to display the current RADIUS authentication client.
Syntax	show auth_client
Description	This command is used to display the current RADIUS authentication client currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS authentication client:

```
DES-3200-28F:4#show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses          0
radiusAuthClientIdentifier                       D-Link

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

show auth_diagnostics

Purpose	Used to display the current authentication diagnostics.
Syntax	show auth_diagnostics {ports [<portlist>]}
Description	This command is used to display the current authentication diagnostics of the Switch on a per port basis.
Parameters	ports <portlist> – Specifies a range of ports.
Restrictions	None.

Example usage:

To display the current authentication diagnostics for port 1:

```
DES-3200-28:4#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port number      : 1
MAC address: 00-00-07-5D-60-02

EntersConnecting          3
EapLogoffsWhileConnecting 0
EntersAuthenticating      2
SuccessWhileAuthenticating 2
TimeoutsWhileAuthenticating 0
FailWhileAuthenticating   0
ReauthsWhileAuthenticating 0
EapStartsWhileAuthenticating 0
EapLogoffWhileAuthenticating 0
ReauthsWhileAuthenticated 0
EapStartsWhileAuthenticated 1
EapLogoffWhileAuthenticated 0
BackendResponses          4
BackendAccessChallenges   2
BackendOtherRequestsToSupplicant 0
BackendNonNakResponsesFromSupplicant 2
BackendAuthSuccesses      2
BackendAuthFails          0
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

show auth_session_statistics

Purpose	Used to display the current authentication session statistics.
Syntax	show auth_session_statistics {ports <portlist all>}
Description	This command is used to display the current authentication session statistics of the Switch on a per port basis.
Parameters	ports <portlist> – Specifies a range of ports. all – Specifies that all ports will be viewed.
Restrictions	None.

Example usage:

To display the current authentication session statistics for port 16:

```
DES-3200-28:4#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port number      : 1
MAC address: 00-00-07-5D-60-02

SessionOctetsRx          7808
SessionOctetsTx          469102741
SessionFramesRx          122
SessionFramesTx          4196211
SessionId                ether1_2-1
SessionAuthenticMethod   Remote Authentication Server
SessionTime               70803
SessionTerminateCause    NotTerminatedYet
SessionUserName           456
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

show auth_statistics

Purpose	Used to display the current authentication statistics.
Syntax	show auth_statistics {ports <portlist>}
Description	This command is used to display the current authentication statistics of the Switch on a per port basis.
Parameters	ports <portlist> – Specifies a range of ports.
Restrictions	None.

Example usage:

To display the current authentication statistics for port 1:

```
DES-3200-28:4#show auth_statistics ports 1
Command: show auth_statistics ports 1

Port number : 1
MAC address: 00-00-07-5D-60-02

EapolFramesRx           6
EapolFramesTx           7
EapolStartFramesRx      2
EapolReqIdFramesTx      3
EapolLogoffFramesRx     0
EapolReqFramesTx        2
EapolRespIdFramesRx     2
EapolRespFramesRx       2
InvalidEapolFramesRx    0
EapLengthErrorFramesRx  0

LastEapolFrameVersion   1
LastEapolFrameSource     00-00-07-5D-60-02
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

create 802.1x user	
Purpose	Used to create a new 802.1X user.
Syntax	create 802.1x user <username 15>
Description	This command is used to create new 802.1X users.
Parameters	<username 15> – A username of up to 15 alphanumeric characters in length.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an 802.1X user:

```
DES-3200-28:4#create 802.1x user ctsnow
Command: create 802.1x user ctsnow

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

DES-3200-28:4#
```

show 802.1x user	
Purpose	Used to display the 802.1X user accounts on the Switch.

show 802.1x user

Syntax	show 802.1x user
Description	This command is used to display the 802.1X Port-based or Host-based Network Access control local users currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view 802.1X users currently configured on the Switch:

```
DES-3200-28:4#show 802.1x user
Command: show 802.1x user

Index  UserName
----  -
1      ctsnow

Total Entries: 1

DES-3200-28:4#
```

delete 802.1x user

Purpose	Used to delete an 802.1X user account on the Switch.
Syntax	delete 802.1x user <username 15>
Description	This command is used to delete the 802.1X Port-based or Host-based Network Access control local users currently configured on the Switch.
Parameters	<username 15> – A username can be as many as 15 alphanumeric characters.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete 802.1X users:

```
DES-3200-28:4#delete 802.1x user ctsnow
Command: delete 802.1x user ctsnow

Success.

DES-3200-28:4#
```

ACCESS CONTROL LIST (ACL) COMMANDS

The Switch implements Access Control Lists that enable the Switch to deny network access to specific devices or device groups based on IP settings and MAC address.

The Access Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create access_profile	[ethernet {vlan {<hex 0x0-0x0fff>} source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type } (1) ip {vlan {<hex 0x0-0x0fff>} source_ip_mask <netmask> destination_ip_mask <netmask> dscp [[icmp {type code} igmp {type} tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin} (1)]] udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> } protocol_id_mask<0x0-0xff> }] (1) packet_content_mask {destination_mac <macmask> source_mac <macmask> c_tag <hex 0x0-0xffff> s_tag <hex 0x0-0xffff> offset1 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset2 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset3 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset4 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset5 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset6 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset7 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset8 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset9 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset10 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset11 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> } (1)] ipv6 { class flowlabel source_ipv6_mask< ipv6mask ::-::FFF:FFF:FFF> [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> }] }] profile_id <value 1-512>
delete access_profile	[profile_id <value 1-512> all]
config access_profile	[profile_id <value 1-512>] [add access_id [auto_assign <value 1-65535>] [ethernet {[vlan <vlan_name 32> vlan_id <vid>] {mask <hex 0x0-0x0fff>} source_mac <macaddr> {mask <macmask>} destination_mac <macaddr> {mask <macmask>} 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>} (1) ip {[vlan <vlan_name 32> vlan_id <vid>] {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 } (1)]] udp {src_port <value 0-65535> dst_port <value 0-65535> } protocol_id <value 0-255> } (1)]] packet_content {destination_mac <macaddr>{mask<macmask>} source_mac <macaddr> {mask <macmask>} c_tag <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} s_tag <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset1 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset2 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset3 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset4 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset5 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset6 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset7 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset8 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset9 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset10 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset11 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} } ipv6 {class <value 0-255> flowlabel <hex 0x0-0xffff> source_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>}} (1)]] [port [<portlist> all]] [permit {priority<value 0-7> {replace_priority} replace_dscp_with <value0-63>} counter [enable disable]] deny mirror] { time_range <range_name 32>} delete access_id <value 1-65535>]
show access_profile	{profile_id <value 1-512>}
enable cpu_interface_filtering	
disable cpu_interface_filtering	

Command	Parameters
create cpu access_profile profile_id	<value 1-3> [ethernet {vlan source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type} (1) ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code } igmp {type } tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin} (1)] } udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>} } (1) packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> } (1) ipv6 [{ class flowlabel source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask>} (1)]
delete cpu access_profile	profile_id <value 1-3>
config cpu access_profile profile_id	profile_id <value 1-3> [add access_id <value 1-5>[ethernet {vlan <vlan_name 32> source_mac <macaddr> destination_mac <macaddr> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>} (1) ip {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> flag [all { urg ack psh rst syn fin} (1)] } udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}}] (1) 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> } (1) ipv6 [{ class <value 0-255> flowlabel <hex 0x0-0xffff>} source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr>}] port [<portlist> all] [permit deny] {time_range <range_name 32>} delete access_id <value 1-5>]
show cpu access_profile	profile_id <value 1-3>

Access profiles allow users to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header.

Creating an access profile is divided into two basic parts. First, an access profile must be created using the create access_profile command. For example, if users want to deny all traffic to the subnet 10.42.73.0 to 10.42.73.255, users must first create an access profile that instructs the Switch to examine all of the relevant fields of each frame.

First create an access profile that uses IP addresses as the criteria for examination:

```
create access_profile ip source_ip_mask 255.255.255.0 profile_id 1
```

Here we have created an access profile that will examine the IP field of each frame received by the Switch. Each source IP address the Switch finds will be combined with the source_ip_mask with a logical AND operation. The profile_id parameter is used to give the access profile an identifying number – in this case, 1 – and it is used to assign a priority in case a conflict occurs. The profile_id establishes a priority within the list of profiles. A lower profile_id gives the rule a higher priority. In case of a conflict in the rules entered for different profiles, the rule with the highest priority (lowest profile_id) will take precedence. See below for information regarding limitations on access profiles and access rules.

The deny parameter instructs the Switch to filter any frames that meet the criteria – in this case, when a logical AND operation between an IP address specified in the next step and the ip_source_mask match.

The default for an access profile on the Switch is to permit traffic flow. If users want to restrict traffic, users must use the deny parameter.

Now that an access profile has been created, users must add the criteria the Switch will use to decide if a given frame should be forwarded or filtered. We will use the config access_profile command to create a new rule that defines the criteria we want. Let's further specify in the new rule to deny access to a range of IP addresses through an individual port: Here, we want to filter any packets that have an IP source address between 10.42.73.0 and 10.42.73.255, and specify the port that will not be allowed:

```
config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny
```

We use the profile_id 1 which was specified when the access profile was created. The add parameter instructs the Switch to add the criteria that follows to the list of rules that are associated with access profile 1. For each rule entered into the access profile,

users can assign an access_id that identifies the rule within the list of rules. The access_id is an index number only and does not effect priority within the profile_id. This access_id may be used later if users want to remove the individual rule from the profile.

The ip parameter instructs the Switch that this new rule will be applied to the IP addresses contained within each frame's header. source_ip tells the Switch that this rule will apply to the source IP addresses in each frame's header. The IP address 10.42.73.1 will be combined with the source_ip_mask 255.255.255.0 to give the IP address 10.42.73.0 for any source IP address between 10.42.73.0 to 10.42.73.255. Finally the restricted port - port number 7 - is specified.

Each command is listed, in detail, in the following sections:

create access_profile

Purpose	Used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	<pre>create access_profile [ethernet {vlan {<hex 0x0-0x0fff>} source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type} (1) ip {vlan {<hex 0x0-0x0fff>} source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp { type code } igmp {type} tcp { src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all { urg ack psh rst syn fin } (1)] } udp { src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> protocol_id_mask<0x0-0xff> }] } (1) packet_content_mask {destination_mac <macmask> source_mac <macmask> c_tag <hex 0x0-0xffff> s_tag <hex 0x0-0xffff> offset1 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset2 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset3 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset4 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset5 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset6 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset7 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset8 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset9 [I2 I3 I4] <value 0-31> <hex 0x0- 0xffff> offset10 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> offset11 [I2 I3 I4] <value 0-31> <hex 0x0-0xffff> } (1)] ipv6 {class flowlabel source_ipv6_mask< ipv6mask ::- ::FFF:FFF:FFF:FFF> [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> }] }] profile_id <value 1-512></pre>
Description	This command is used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Parameters	<p>ethernet – Specifies that the Switch will examine the layer 2 part of each packet header.</p> <p>vlan – Specifies a VLAN mask. Only the last 12 bits of the mask will be considered.</p> <p>source_mac <macmask> – Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format.</p> <p>destination_mac <macmask> – Specifies a MAC address mask for the destination MAC address.</p> <p>802.1p – Specifies that the Switch will examine the 802.1p priority value in the frame's header.</p> <p>ethernet_type – Specifies that the Switch will examine the Ethernet type value in each frame's header.</p> <p>ip – Specifies that the Switch will examine the IP fields in each frame's header.</p> <p>vlan – Specifies a VLAN mask. Only the last 12 bits of the mask will be considered.</p> <p>source_ip_mask <netmask> – Specifies an IP address mask for the source IP address.</p> <p>destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.</p> <p>dscp – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.</p> <p>icmp – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <p>type – Specifies that the Switch will examine each frame's ICMP Type field.</p> <p>code – Specifies that the Switch will examine each frame's ICMP Code field.</p> <p>igmp – Specifies that the Switch will examine each frame's Internet Group Management</p>

create access_profile

Protocol (IGMP) field.

type – Specifies that the Switch will examine each frame's IGMP Type field.

tcp – Specifies that the Switch will examine each frames Transport Control Protocol (TCP) field.

src_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.

dst_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.

flag_mask – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose among all, urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize) and fin (finish).

udp – Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field.

src_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.

dst_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.

protocol_id_mask – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.

ipv6 - Specifies IPv6 filtering mask.

class – Specifies the IPv6 class.

flowlabel – Specifies the IPv6 flow label.

source_ipv6_mask – Specifies an IPv6 source submask. The device only supports filtering of the last 44 bits (LSB) of the source IPv6 address.

src_port_mask – Specifies an IPv6 L4 (TCP/UDP) source port submask.

dst_port_mask - Specifies an IPv6 L4 (TCP/UDP) destination port submask.

packet_content_mask – A maximum of 11 offsets can be specified. Each offset defines two bytes of data, which is identified as a single UDF field. The offset reference is also configurable. It can be defined to start at the end of a tag, the end of an ether type or the end of an IP header. To qualify the fields before the end of a tag, the destination address, source address, and the VLAN tags are also included.

source_mac – Specifies the source MAC mask.

destination_mac – Specifies the destination MAC mask.

c_tag – Specifies the 16-bit inner VLAN tag of the packet to mask. This constitutes the 3-bit PCP, 1-bit CFI and 12-bit VID fields.

s_tag – Specifies the 16-bit outer VLAN tag of the packet to mask. This constitutes the 3-bit PCP, 1-bit CFI and 12-bit VID fields.

offset1 – offset11 - Defines the UDF fields to which the device will filter. Each UDF field is a 2-byte data which is n bytes away from the offset reference (where n is the offset value). The offset can range from 0 up to 31. The offset reference can be either of the following:

I2 – The offset will start counting from the byte after the end of the VLAN tags (start of ether type).

I3 – The offset will start counting right after the ether type field. The packet must have a valid L2 header and a recognizable ether type in order to be recognized.

I4 – The offset will start counting right after the end of ip header. The packet must have a valid IP header in order to be recognized.

Example: "offset1 I2 0 0xFFFF" will mask the first 2 bytes of the ether type.

profile_id <value 1-512> – Sets the relative priority for the profile. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 to 512.

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To create an access list rule:

```
DES-3200-28:4#create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp profile_id 101
Command: create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp permit profile_id 101

Success.

DES-3200-28:4#
```

delete access_profile	
Purpose	Used to delete a previously created access profile.
Syntax	delete access_profile [profile_id <value 1-512> all]
Description	This command is used to delete a previously created access profile on the Switch.
Parameters	<p>profile_id <value 1-512> – Enter an integer between 1 and 512 that is used to identify the access profile that will be deleted with this command. This value is assigned to the access profile when it is created with the create access_profile command. The user may enter a profile ID number between 1 and 512.</p> <p>all – Specifies all access list profiles will be deleted.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3200-28:4# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DES-3200-28:4#
```

config access_profile

Purpose	Used to configure an access profile on the Switch and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the create access_profile command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	<pre>config access_profile [profile_id <value 1-512>] [add access_id [auto_assign <value 1-65535>] [ethernet {[vlan <vlan_name 32> vlan_id <vid> } {mask <hex 0x0-0x0fff>} source_mac <macaddr> {mask <macmask>} destination_mac <macaddr> {mask <macmask>} 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>} (1) ip {[vlan <vlan_name 32> vlan_id <vid>} {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 } (1)] } udp {src_port <value 0-65535> dst_port <value 0-65535> } protocol_id <value 0-255> } (1)] packet_content {destination_mac <macaddr>{mask<macmask>} source_mac <macaddr> {mask <macmask>} c_tag <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} s_tag <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset1 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset2 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset3 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset4 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset5 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset6 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset7 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset8 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} offset9 <hex 0x0-</pre>

config access_profile

```
0xffff> {mask <hex 0x0-0xffff>} | offset10 <hex 0x0-0xffff> {mask <hex 0x0-0xffff>} | offset11
<hex 0x0-0xffff> {mask <hex 0x0-0xffff>} } | ipv6 {class <value 0-255> | flowlabel <hex 0x0-
0xffff> | source_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>}} (1) ]}]
[port [<portlist>|all]] [permit {priority<value 0-7> {replace_priority} | replace_dscp_with <value0-
63>| counter [enable | disable] } | deny | mirror ] { time_range <range_name 32>} | delete
access_id <value 1-65535>]
```

Description This command is used to configure an access profile on the Switch and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the create access_profile command, above.

Parameters profile_id <value 1-512> – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the create access_profile command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 and 512.

add access_id <value 1-65535> – Adds an additional rule to the above specified access profile. The value is used to index the rule created. For information on number of rules that can be created for a given port, please see the introduction to this chapter.

auto_assign – Choose this parameter to configure the Switch to automatically assign a numerical value (between 1 and 65535) for the rule being configured.

ethernet – Specifies that the Switch will look only into the layer 2 part of each packet.

vlan <vlan_name 32> – Specifies that the access profile will only apply to the VLAN with this name.

vlan_id <vid> – Specifies that the access profile will only apply to packets belonging to the VLAN with this ID.

source_mac <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address.

destination_mac <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address.

802.1p <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.

ethernet_type <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

Parameters ip – Specifies that the Switch will look into the IP fields in each packet.

vlan <vlan_name 32> – Specifies that the access profile will only apply to the VLAN with this name.

vlan_id <vid> – Specifies that the access profile will only apply to packets belonging to the VLAN with this VLAN ID.

source_ip <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address.

destination_ip <ipaddr> – Specifies that the access profile will apply to only packets with this destination IP address.

dscp <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.

icmp – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.

type – Specifies that the Switch will examine each frame's ICMP Type field.

code – Specifies that the Switch will examine each frame's ICMP Code field.

igmp – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

config access_profile

type – Specifies that the Switch will examine each frame's IGMP Type field.

tcp – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.

src_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.

dst_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.

flag – Enter the type of TCP flag to be matched.

all: all flags are selected.

urg: TCP control flag (urgent)

ack: TCP control flag (acknowledgement)

psh: TCP control flag (push)

rst: TCP control flag (reset)

syn: TCP control flag (synchronize)

fin: TCP control flag (finish)

udp – Specifies that the Switch will examine the Universal Datagram Protocol (UDP) field in each packet.

src_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.

dst_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.

protocol_id <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.

ipv6 - Specifies IPv6 filtering mask.

class – Specifies the IPv6 class.

flowlabel – Specifies the IPv6 flow label.

source_ipv6_mask – Specifies an IPv6 source address.

src_port_mask – Specifies an IPv6 L4 (TCP/UDP) source port submask.

dst_port_mask – Specifies an IPv6 L4 (TCP/UDP) destination port submask.

packet_content – A maximum of 11 offsets can be specified. Each offset defines two bytes of data, which is identified as a single UDF field. The offset reference is also configurable. It can be defined to start at the end of a tag, the end of an ether type or the end of an IP header. To qualify the fields before the end of a tag, the destination address, source address, and the VLAN tags are also included.

source_mac – Specifies that the access profile will only apply to packets with this source MAC address.

destination_mac – Specifies that the access profile will only apply to packets with this destination MAC address.

c_tag – Specifies the 16-bit inner VLAN tag of the packet to match. This constitutes the 3-bit PCP, 1-bit CFI and 12-bit VID fields.

s_tag – Specifies the 16-bit outer VLAN tag of the packet to match. This constitutes the 3-bit PCP, 1-bit CFI and 12-bit VID fields.

offset1 – offset11 – Specifies the data to match for each match UDF field data defined in the profile.

Example: If offset1 defined as "offset1 0 L2 0x00FF" is defined in the profile, and in this command the data specified is "offset1 0x00AA", then the switch will look at the second byte of the ether type. If the byte matches 0xAA, then the device will process the packet according to the configured action.

Parameters

port <portlist> – Specifies the port number on the Switch to permit or deny access for the rule. The user can also configure "all" to specify all ports.

permit – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

priority <value 0-7> – This parameter is specified if you want to re-write the 802.1p user priority

config access_profile

value set in the packet, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.

replace_priority – Enter this parameter if you want to re-write the 802.1p user priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

replace_dscp_with – Specifies that DSCP of the outgoing packet will be marked by the new value.

counter – Specifies whether the counter feature will be enabled or disabled. The is optional. The default is disable. If the rule is not bound with a flow meter, then all packets matched will be counted. If the rule is bound with a flow meter, the counter is overridden.

deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.

mirror – Specifies the packets that match the access profile are sent the copied one to the mirror port.

time_range <range_name 32> – Choose this parameter and enter the name of the Time Range settings that has been previously configured using the config time_range command. This will set specific times when this access rule will be enabled or disabled on the Switch.

mask - These options provides an additional mask for each field. This additional mask should be subset of the field mask defined by the profile. The final mask is the result of the AND operation of the profile mask and this per rule mask.

delete access_id <value 1-65535> – Use this command to delete a specific ACL rule from the Ethernet profile, IP profile or packet_content profile. Up to 512 rules may be specified for all access profiles.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the access profile with the profile ID of 1 to filter frames on port 7 that have IP addresses in the range between 10.42.73.0 to 10.42.73.255:

```
DES-3200-28:4# config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1
port 7 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7
deny
Success.
DES-3200-28:4#
```

show access_profile

Purpose Used to display the currently configured access profiles on the Switch.

Syntax show access_profile {profile_id <value 1-512>}

Description This command is used to display the currently configured access profiles.

Parameters profile_id <value 1-512> – Specify the profile id to display only the access rules configuration for a single profile ID. The user may enter a profile ID number between 1 and 512.

Restrictions None.

Example usage:

To display all of the currently configured access profiles on the Switch:

```

DES-3200-28:4#show access_profile
Command: show access_profile

Access Profile Table

=====
Profile ID: 101                               Type: IPv4 Frame Filter - ICMP
=====
Masks  Option
VLAN    Source IP    Dest. IP    DSCP Prot
-----
0xFFF  20.0.0.0    10.0.0.0    ICMP
=====

Total Profile Entries: 1

Total Used Rule Entries: 0

Total Unused Rule Entries: 512

DES-3200-28:4#
    
```

create cpu access_profile

Purpose	Used to create an access profile specifically for CPU Interface Filtering on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config cpu access_profile command, below.
Syntax	create cpu access_profile profile_id <value 1-3> [ethernet {vlan source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type} (1) ip { vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code } igmp {type } tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin} (1)] } udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} (1) packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> } (1) ipv6 [{ class flowlabel source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask>} (1)]
Description	This command is used to create an access profile used only for CPU Interface Filtering. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config cpu access_profile command, below.
Parameters	<p>ethernet – Specifies that the Switch will examine the layer 2 part of each packet header.</p> <p>vlan – Specifies that the Switch will examine the VLAN part of each packet header.</p> <p>source_mac <macmask> – Specifies to examine the source MAC address mask.</p> <p>destination_mac <macmask> – Specifies to examine the destination MAC address mask.</p> <p>802.1p – Specifies that the Switch will examine the 802.1p priority value in the frame's header.</p> <p>ethernet_type – Specifies that the Switch will examine the Ethernet type value in each frame's header.</p> <p>ip – Specifies that the Switch will examine the IP fields in each frame's header.</p> <p>vlan – Specifies a VLAN mask.</p>

create cpu access_profile

source_ip_mask <netmask> – Specifies an IP address mask for the source IP address.

destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.

dscp – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.

icmp – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.

type – Specifies that the Switch will examine each frame's ICMP Type field.

code – Specifies that the Switch will examine each frame's ICMP Code field.

igmp – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.

type – Specifies that the Switch will examine each frame's IGMP Type field.

tcp – Specifies that the Switch will examine each frames Transport Control Protocol (TCP) field.

src_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.

dst_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.

flag_mask [all | {urg | ack | psh | rst | syn | fin}] – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between all, urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize) and fin (finish).

udp – Specifies that the switch will examine each frame's Universal Datagram Protocol (UDP) field.

src_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.

dst_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.

protocol_id_mask <hex 0x0-0xff> – Specifies that the Switch will examine each frame's Protocol ID field using the hex form entered here.

user_define_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.

packet_content_mask – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows:

offset_0-15 – Enter a value in hex form to mask the packet from byte 0 to byte 15.

offset_16-31 – Enter a value in hex form to mask the packet from byte 16 to byte 31.

offset_32-47 – Enter a value in hex form to mask the packet from byte 32 to byte 47.

offset_48-63 – Enter a value in hex form to mask the packet from byte 48 to byte 63.

offset_64-79 – Enter a value in hex form to mask the packet from byte 64 to byte 79.

ipv6 – Denotes that IPv6 packets will be examined by the Switch for forwarding or filtering based on the rules configured in the config access_profile command for IPv6. IPv6 packets may be identified by the following:

class – Entering this parameter will instruct the Switch to examine the class field of the IPv6 header that is similar to the Type of Service (ToS) or Precedence bits field in Ipv4.

flowlabel – Entering this parameter will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real-time service packets.

source_ipv6_mask <ipv6mask> – Specifies an IP address mask for the source IPv6 address.

destination_ipv6_mask <ipv6mask> – Specifies an IP address mask for the destination IPv6 address.

profile_id <value 1-3> – Enter an integer between 1 and 3 that is used to identify the CPU access profile to be created with this command.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To create a CPU access profile:

```
DES-3200-28:4# create cpu access_profile profile_id 1 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 1 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DES-3200-28:4#
```

delete cpu access_profile

Purpose	Used to delete a previously created CPU access profile.
Syntax	delete cpu access_profile profile_id <value 1-3>
Description	This command is used to delete a previously created CPU access profile.
Parameters	profile_id <value 1-3> – Enter an integer between 1 and 3 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the create cpu access_profile command.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DES-3200-28:4#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3200-28:4#
```

config cpu access_profile

Purpose	Used to configure a CPU access profile used for CPU Interface Filtering and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the create cpu access_profile command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config cpu access_profile command, below.
Syntax	config cpu access_profile profile_id <value 1-3> [add access_id <value 1-5>[ethernet {vlan <vlan_name 32> source_mac <macaddr> destination_mac <macaddr > 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>} (1) ip{vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> flag [all { urg ack psh rst syn fin} (1)]} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}}] (1) 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> } (1) ipv6 {[class <value 0-255> flowlabel <hex 0x0-0xffff>} source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr>}}]port [<portlist> all] [permit deny] {time_range <range_name 32>} delete access_id <value

config cpu access_profile

1-5>]

Description	This command is used to configure a CPU access profile for CPU Interface Filtering and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the create cpu access_profile command, above.
Parameters	<p>profile_id <value 1-3> – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the create access_profile command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority.</p>
Parameters	<p>add access_id <value 1-5> – Adds an additional rule to the above specified access profile. The value is used to index the rule created.</p> <p>ethernet – Specifies that the Switch will look only into the layer 2 part of each packet.</p> <p> vlan <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN.</p> <p> source_mac <macaddr> – Specifies that the access profile will apply to this source MAC address.</p> <p> destination_mac <macaddr> – Specifies that the access profile will apply to this destination MAC address.</p> <p> ethernet_type <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.</p> <p>ip – Specifies that the Switch will look into the IP fields in each packet.</p> <p> vlan <vlan_name 32> – Specifies that the access profile will apply to only this VLAN.</p> <p> source_ip <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address.</p> <p> destination_ip <ipaddr> – Specifies that the access profile will apply to only packets with this destination IP address.</p> <p> dscp <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header</p> <p> icmp – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.</p> <p> type – Specifies that the Switch will examine each frame's ICMP Type field.</p> <p> code – Specifies that the Switch will examine each frame's ICMP Code field.</p> <p> igmp – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.</p> <p> type – Specifies that the Switch will examine each frame's IGMP Type field.</p> <p> tcp – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.</p> <p> src_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.</p> <p> dst_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.</p> <p>flag- Enter the type of TCP flag to be matched.</p> <p> all: All flags are selected</p> <p> urg: TCP control flag (urgent)</p> <p> ack: TCP control flag (acknowledgement)</p> <p> psh: TCP control flag (push)</p> <p> rst: TCP control flag (reset)</p> <p> syn: TCP control flag (synchronize)</p> <p> fin: TCP control flag (finish)</p> <p>udp – Specifies that the Switch will examine the User Datagram Protocol (UDP) field within each packet.</p>

config cpu access_profile

src_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.

dst_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.

protocol_id <value 0-255> – Specifies that the Switch will examine the protocol field in each packet, and if this field contains the value entered here, apply the following rules:

user_define_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.

ipv6 – Denotes that IPv6 packets will be examined by the Switch for forwarding or filtering based on the rules configured in the config access_profile command for IPv6. IPv6 packets may be identified by the following:

class <value 0-255> – Entering this parameter will instruct the Switch to examine the class field of the IPv6 header that is similar to the Type of Service (ToS) or Precedence bits field in Ipv4.

flowlabel <hex 0x0-ffff> – Entering this parameter will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real-time service packets.

source_ipv6_mask <ipv6mask> – Specifies an IP address mask for the source IPv6 address.

destination_ipv6_mask <ipv6mask> – Specifies an IP address mask for the destination IPv6 address.

packet_content_mask – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows:

offset_0-76 - Enter a value in hex form to mask the packet from byte 0 to byte 76.

<portlist> – Specifies a port or range of ports to be configured.

permit | deny – Specify that the packet matching the criteria configured with command will either be permitted entry to the cpu or denied entry to the CPU.

time_range <range_name 32> – Choose this parameter and enter the name of the Time Range settings that has been previously configured using the config time_range command. This will set specific times when this access rule will be enabled or disabled on the Switch.

delete access_id <value 1-5> – Use this to remove a previously created access rule in a profile ID.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure CPU access list entry:

```
DES-3200-28:4#config cpu access_profile profile_id 3 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 all deny
```

```
Command: config cpu access_profile profile_id 3 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 all deny
```

Success.

```
DES-3200-28:4#
```

delete cpu access_profile

Purpose Used to delete a previously created CPU access profile.

Syntax delete cpu access_profile profile_id <value 1-3>

Description This command is used to delete a previously created CPU access profile.

Parameters profile_id <value 1-3> – Enter an integer between 1 and 3 that is used to identify the CPU access profile to be deleted with this command. This value

delete cpu access_profile

is assigned to the access profile when it is created with the create cpu access_profile command.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DES-3200-28:4#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3200-28:4#
```

show cpu access_profile

Purpose Used to view the CPU access profile entry currently set in the Switch.

Syntax show cpu access_profile profile_id <value 1-3>

Description This command is used view the current CPU interface filtering entries set on the Switch.

Parameters profile_id <value 1-3> – Enter an integer between 1 and 3 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the create cpu access_profile command.

Restrictions None.

Example usage:

To show the CPU filtering state on the Switch:

```

DES-3200-28:4#show cpu_access_profile
Command: show cpu_access_profile

CPU Interface Filtering state: Enabled

Access Profile Table

=====
Profile ID: 1                               Type: IPv4 Frame Filter - ICMP
=====
Owner: ACL
Masks Option
VLAN          Source IP      Dest. IP      DSCP Prot Type Code
-----
0xFFF         20.0.0.0      10.0.0.0      ICMP
-----

Access ID : 3
Ports      : 1-10
Mode       : Deny

VLAN Name    Source IP      Dest. IP      DSCP Prot Type Code
Mask         Mask          Mask
-----
default (0x1) 20.0.0.0      10.0.0.0      3    ICMP 11  32
-----

Total Profile Entries: 1

Total Rule Entries: 1
    
```

enable cpu_interface_filtering	
Purpose	Used to enable CPU interface filtering on the Switch.
Syntax	enable cpu_interface_filtering
Description	This command is used, in conjunction with the disable cpu_interface_filtering command below, to enable and disable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To enable CPU interface filtering:

```

DES-3200-28:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3200-28:4#
    
```

disable cpu_interface_filtering	
Purpose	Used to disable CPU interface filtering on the Switch.

disable cpu_interface_filtering

Syntax	disable cpu_interface_filtering
Description	This command is used, in conjunction with the enable cpu_interface_filtering command above, to enable and disable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To disable CPU filtering:

```
DES-3200-28:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-3200-28:4#
```

TIME RANGE COMMANDS

The Time Range commands are used in conjunction with the Access Profile commands listed in the previous chapter to determine a starting point and an ending point, based on days of the week, when an Access Profile configuration will be enabled on the Switch. Once configured here, the time ranges will be applied to an access profile rule using the `config access_profile profile_id` command.



NOTE: The Time Range commands are based on the time settings of the Switch. Make sure to configure the time for the Switch appropriately for these commands using commands listed in the following chapter, Time and SNTP Commands.

The Time Range commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
<code>config time_range</code>	<code><range_name 32> [hours start_time <hh:mm:ss> end_time <hh:mm:ss> weekdays <daylist> delete]</code>
<code>show time_range</code>	

Each command is listed, in detail, in the following sections.

config time_range

Purpose	Used to configure a time range in which an access profile rule is to be enabled.
Syntax	<code>config time_range <range_name 32> [hours start_time <hh:mm:ss> end_time <hh:mm:ss> weekdays <daylist> delete]</code>
Description	This command is to be used in conjunction with an access profile rule to determine a period of time when an access profile and an associated rule are to be enabled on the Switch. Remember, this time range can only be applied to one period of time and also, it is based on the time set on the Switch.
Parameters	<p><code><range_name 32></code> – Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the <code>config access_profile profile_id</code> command to identify the access profile and associated rule to be enabled for this time range.</p> <p><code>hours</code> – This parameter is used to set the time in the day that this time range is to be set using the following parameters:</p> <ul style="list-style-type: none"> <code>start time <hh:mm:ss></code> – Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. <code>end time <hh:mm:ss></code> – Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system. <p><code>weekdays</code> – Use this parameter to determine the days of the week to set this time range.</p> <p><code><daylist></code> – The user may set the days of the week here to set this time range in the three letter format (mon, tue, wed...). To specify a day range, separate the daylist using a dash (mon-fri would mean Monday through Friday). To specify a list of days in a week, separate the daylist using a comma, with no spaces (mon,tue,fri would mean Monday, Tuesday and Friday).</p>

config time_range

delete – Use this parameter to delete a previously configured time range from the system.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the time range time1 to be between 6:30 a.m. and 9:40 p.m., Monday to Friday:

```
DES-3200-28:4#config time_range time1 hours start_time 6:30:00 end_time
21:40:00 weekdays mon-fri
Command: config time_range time1 hours start_time 6:30:00 end_time 21:40:00
weekdays mon-fri

Success.

DES-3200-28:4#
```

show time_range

Purpose Used to view the current configurations of the time range set on the Switch.

Syntax show time_range

Description This command is used to display the currently configured time range(s) set on the Switch.

Parameters None.

Restrictions None.

Example usage:

To view the current time range settings:

```
DES-3200-28:4#show time_range
Command: show time_range

Time Range Information
-----
Range Name      : time1
Selected       : Mon,Tue,Wed,Thu,Fri
Start time     : 06:30:00
End time       : 21:40:00
Associated ACL Entries:
Associated CPU interface Entries:

Total time range :1

DES-3200-28:4#
```

SAFEGUARD ENGINE COMMANDS

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the CPU utilization beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter an Exhausted mode. When in this mode, the Switch will perform the following tasks to minimize the CPU usage:

It will limit bandwidth of receiving ARP packets.

It will limit the bandwidth of IP packets received by the Switch.

IP packets may also be limited by the Switch by configuring only certain IP addresses to be accepted. This method can be accomplished through the create trusted_host explained in the previous section. Once the user configures these acceptable IP addresses, other packets containing different IP addresses will be dropped by the Switch, thus limiting the bandwidth of IP packets

The Safeguard Engine commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config safeguard_engine	{state [enable disable] utilization {rising <value 20-100> falling <value 20-100>} (1) trap_log [enable disable] mode [strict fuzzy]} (1)
show safeguard_engine	

Each command is listed, in detail, in the following sections.

config safeguard_engine

Purpose	Used to configure ARP storm control for system.
Syntax	{state [enable disable] utilization {rising <value 20-100> falling <value 20-100>} (1) trap_log [enable disable] mode [strict fuzzy]} (1)
Description	This command is used to configure Safeguard Engine to minimize the effects of an ARP storm.
Parameters	<p>state [enable disable] – Select the running state of the Safeguard Engine function as enable or disable.</p> <p>cpu_utilization – Select this option to trigger the Safeguard Engine function to enable based on the following determinates:</p> <p>rising <value 20-100> – The user can set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises to this percentage, the Safeguard Engine mechanism will initiate.</p> <p>falling <value 20-100> – The user can set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to this percentage, the Safeguard Engine mechanism will shut down.</p> <p>trap_log [enable disable] – Choose whether to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.</p> <p>mode [strict fuzzy] – Toggle between strict and fuzzy mode.</p> <p>strict – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided.</p> <p>fuzzy – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth</p>

config safeguard_engine

to all traffic flows.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the safeguard engine for the Switch:

```
DES-3200-28:4#config safeguard_engine state enable utilization rising 45
Command: config safeguard_engine state enable utilization rising 45

Success.

DES-3200-28:4#
```

show safeguard_engine

Purpose	Used to display current Safeguard Engine settings.
Syntax	show safeguard_engine
Description	This command is used to list the current status and type of the Safeguard Engine settings currently configured.
Parameters	None.
Restrictions	None.

Example usage:

To display the safeguard engine status:

```
DES-3200-28:4#show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State          : Disabled
Safeguard Engine Current Status : Normal mode
=====
CPU Utilization Information:
Rising Threshold   : 30%
Falling Threshold  : 20%
Trap/Log State     : Disabled
Mode               : Fuzzy

DES-3200-28:4#
```

TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows users to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied.

The Traffic Segmentation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table

Command	Parameters
config traffic_segmentation	<portlist> forward_list [null <portlist>]
show traffic_segmentation	{<portlist>}

Each command is listed, in detail, in the following sections.

config traffic_segmentation	
Purpose	Used to configure traffic segmentation on the Switch.
Syntax	config traffic_segmentation <portlist> forward_list [null <portlist>]
Description	This command is used to configure traffic segmentation on the Switch.
Parameters	<p><portlist> – Specifies a port or range of ports that will be configured for traffic segmentation.</p> <p>forward_list – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.</p> <p>null – No ports are specified</p> <p><portlist> – Specifies a range of ports for the forwarding list. This list must be on the same Switch previously specified for traffic segmentation (i.e. following the <portlist> specified above for config traffic_segmentation).</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure ports 1 through 10 to be able to forward frames to port 11 through 15:

```
DES-3200-28:4#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DES-3200-28:4#
```

show traffic_segmentation	
Purpose	Used to display the current traffic segmentation configuration on the Switch.

show traffic_segmentation

Syntax	show traffic_segmentation {<portlist>}
Description	This command is used to display the current traffic segmentation configuration on the Switch.
Parameters	<portlist> – Specifies a port or range of ports for which the current traffic segmentation configuration on the Switch will be displayed.
Restrictions	The port lists for segmentation and the forward list must be on the same Switch.

Example usage:

To display the current traffic segmentation configuration on the Switch:

```
DES-3200-28:4#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port      Forward Portlist
-----  -
1         1-28
2         1-28
3         1-28
4         1-28
5         1-28
6         1-28
7         1-28
8         1-28
9         1-28
10        1-28
11        1-28
12        1-28
13        1-28
14        1-28
15        1-28
16        1-28
17        1-28
18        1-28

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

TIME AND SNTP COMMANDS

The Simple Network Time Protocol (SNTP) (an adaptation of the Network Time Protocol (NTP)) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config sntp	{primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>} (1)
show sntp	
enable sntp	
disable sntp	
config time	<date ddmmmyyyy > <time hh:mm:ss >
config time_zone	{operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>}
config dst	[disable repeating {s_week <start_week 1-5,last> s_day <start_day sun-sat> s_mth <start_mth 1-12> s_time <start_time hh:mm> e_week <end_week 1-5,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	

Each command is listed, in detail, in the following sections.

config sntp	
Purpose	Used to setup SNTP service.
Syntax	config sntp {primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>} (1)
Description	This command is used to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable sntp).
Parameters	<p>primary – This is the primary server from which the SNTP information will be taken.</p> <p><ipaddr> – The IP address of the primary server.</p> <p>secondary – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <p><ipaddr> – The IP address for the secondary server.</p> <p>poll-interval <int 30-99999> – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99999 seconds.</p>
Restrictions	Only Administrator-level users can issue this command. SNTP service must be enabled for this command to function (enable sntp).

Example usage:

To configure SNTP settings:


```
DES-3200-28:4#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval
30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DES-3200-28:4#
```

show sntp	
Purpose	Used to display the SNTP information.
Syntax	show sntp
Description	This command is used to display SNTP settings information including the source IP address, time and poll interval.
Parameters	None.
Restrictions	None.

Example usage:

To display SNTP configuration information:

```
DES-3200-28:4#show sntp
Command: show sntp

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

DES-3200-28:4#
```

enable sntp	
Purpose	To enable SNTP server support.
Syntax	enable sntp
Description	This command is used to enable SNTP support. SNTP service must be separately configured (see config sntp). Enabling and configuring SNTP support will override any manually configured system time settings.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command. SNTP settings must be configured for SNTP to function (config sntp).

Example usage:

To enable the SNTP function:

```
DES-3200-28:4#enable sntp
Command: enable sntp

Success.

DES-3200-28:4#
```

disable sntp

Purpose	To disable SNTP server support.
Syntax	disable sntp
Description	This command is used to disable SNTP support. SNTP service must be separately configured (see config sntp).
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SNTP support:

```
DES-3200-28:4#disable sntp
Command: disable sntp

Success.

DES-3200-28:4#
```

config time

Purpose	Used to manually configure system time and date settings.
Syntax	config time <date ddmmyyyy> <time hh:mm:ss>
Description	This command is used to configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<p>date – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003.</p> <p>time – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.</p>
Restrictions	Only Administrator-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
DES-3200-28:4#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3200-28:4#
```

config time_zone	
Purpose	Used to determine the time zone used in order to adjust the system clock.
Syntax	config time_zone {operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>}
Description	This command is used to adjust system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	operator – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT. hour – Select the number of hours different from GMT. min – Select the number of minutes that need to be added or subtracted to adjust the time zone.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DES-3200-28:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3200-28:4#
```

config dst	
Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	config dst [disable repeating {s_week <start_week 1-5,last> s_day <start_day sun-sat> s_mth <start_mth 1-12> s_time start_time hh:mm> e_week <end_week 1-5,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]}]
Description	DST can be enabled and configured using this command. When enabled this will adjust the system clock to comply with any DST requirement. DST adjustment effects system time for both manually configured time and time set using SNTP service.

config dst

disable – Disable the DST seasonal time adjustment for the Switch.

repeating – Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.

annual – Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.

s_week – Configure the week of the month in which DST begins.

<start_week 1-5,last> – The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month.

e_week - Configure the week of the month in which DST ends.

Parameters

<end_week 1-5,last> – The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month.

s_day – Configure the day of the week in which DST begins.

<start_day sun-sat> – The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)

e_day – Configure the day of the week in which DST ends.

<end_day sun-sat> – The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)

s_mth – Configure the month in which DST begins.

<start_mth 1-12> – The month to begin DST expressed as a number.

e_mth – Configure the month in which DST ends.

<end_mth 1-12> – The month to end DST expressed as a number.

s_time – Configure the time of day to begin DST.

<start_time hh:mm> – Time is expressed using a 24-hour clock, in hours and minutes.

e_time – Configure the time of day to end DST.

<end_time hh:mm> – Time is expressed using a 24-hour clock, in hours and minutes.

s_date – Configure the specific date (day of the month) to begin DST.

<start_date 1-31> – The start date is expressed numerically.

e_date – Configure the specific date (day of the month) to begin DST.

<end_date 1-31> – The end date is expressed numerically.

offset [30 | 60 | 90 | 120] – Indicates number of minutes to add or to subtract during the summertime. The possible offset times are 30,60,90,120. The default value is 60

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DES-3200-28:4#config dst repeating s_week 2 s_day tue s_mth 4 s_time
15:00 e_week 2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00
e_week 2 e_day wed e_mth 10 e_time 15:30 offset 30

Success.

DES-3200-28:4#
```

show time

Purpose	Used to display the current time settings and status.
Syntax	show time
Description	This command is used to display system time and date configuration as well as display current system time.
Parameters	None.
Restrictions	None.

Example usage:

To display the time currently set on the Switch's System clock:

```
DES-3200-28:4#show time
Command: show time

Current Time Source : System Clock
Current Time       : 1 Days 01:39:17
Time Zone         : GMT +02:30
Daylight Saving Time: Repeating
Offset in minutes  : 30
  Repeating From   : Apr 2nd Tue 15:00
  To               : Oct 2nd Wed 15:30
  Annual From     : 29 Apr 00:00
  To              : 12 Oct 00:00

DES-3200-28:4#
```

ARP COMMANDS

The ARP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create arprentry	<ipaddr> <macaddr>
config arprentry	<ipaddr> <macaddr>
delete arprentry	{[<ipaddr> all]}
show arprentry	{ipif [System] ipaddress <ipaddr> static}
config arp_aging time	<value 0-65535>
clear arptable	

Each command is listed, in detail, in the following sections.

create arprentry

Purpose	Used to make a static entry into the ARP table.
Syntax	create arprentry <ipaddr> <macaddr>
Description	This command is used to enter an IP address and the corresponding MAC address into the Switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. <macaddr> – The MAC address corresponding to the IP address above.
Restrictions	Only Administrator-level users can issue this command. The Switch supports up to 255 static ARP entries.

Example Usage:

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

```
DES-3200-28:4#create arprentry 10.48.74.121 00-50-BA-00-07-36
Command: create arprentry 10.48.74.121 00-50-BA-00-07-36

Success.

DES-3200-28:4#
```

config arprentry

Purpose	Used to configure a static entry in the ARP table.
Syntax	config arprentry <ipaddr> <macaddr>
Description	This command is used to configure a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the Switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. <macaddr> – The MAC address corresponding to the IP address above.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To configure a static ARP entry for the IP address 10.48.74.12 and MAC address 00:50:BA:00:07:36:

```
DES-3200-28:4#config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

Success.

DES-3200-28:4#
```

delete arpentry	
Purpose	Used to delete a static entry into the ARP table.
Syntax	delete arpentry {[<ipaddr> all]}
Description	This command is used to delete a static ARP entry, made using the create arpentry command above, by specifying either the IP address of the entry or all. Specifying all clears the Switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. all – Deletes all ARP entries.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

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

```
DES-3200-28:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-3200-28:4#
```

config arp_aging time	
Purpose	Used to configure the age-out timer for ARP table entries on the Switch.
Syntax	config arp_aging time <value 0-65535>
Description	This command is used to set the maximum amount of time, in minutes, that an ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	time <value 0-65535> – The ARP age-out time, in minutes. The value may be set in the range of 0-65535 minutes with a default setting of 20 minutes.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```
DES-3200-28:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3200-28:4#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	show arpentry {ipif [System] ipaddress <ipaddr> static}
Description	This command is used to display the current contents of the Switch's ARP table.
Parameters	<p>ipif [System] – The name of the IP interface, the end node or station for which the ARP table entry was made, resides on.</p> <p>ipaddress <ipaddr> – The network address corresponding to the IP interface name above.</p> <p>static – Displays the static entries to the ARP table.</p>
Restrictions	None.

Example Usage:

To display the ARP table:

```
DES-3200-28:4#show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface      IP Address      MAC Address      Type
-----
System         10.0.0.0        FF-FF-FF-FF-FF-FF Local/Broadcast
System         10.6.51.15      00-1D-60-E7-B5-CD Dynamic
System         10.22.8.50      00-80-C8-DF-E8-EE Dynamic
System         10.30.28.112    00-30-28-01-12-02 Dynamic
System         10.39.77.24     08-00-01-43-00-00 Dynamic
System         10.44.8.253     00-44-08-FD-09-09 Dynamic
System         10.53.7.12      00-50-BA-11-11-04 Dynamic
System         10.56.85.10     00-0E-A6-8F-72-EA Dynamic
System         10.67.33.67     00-00-E2-58-DB-CF Dynamic
System         10.71.77.126    00-04-96-20-D5-25 Dynamic
System         10.73.21.11     00-19-5B-EF-78-B5 Local
System         10.73.60.106    00-00-00-11-12-13 Dynamic
System         10.90.90.90     00-21-91-21-34-03 Dynamic
System         10.255.255.255  FF-FF-FF-FF-FF-FF Local/Broadcast

Total Entries  : 14

DES-3200-28:4#
```

clear arptable

Purpose	Used to remove all dynamic ARP table entries.
Syntax	clear arptable

clear arptable

Description	This command is used to remove dynamic ARP table entries from the Switch's ARP table. Static ARP table entries are not affected.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
DES-3200-28:4#clear arptable
Command: clear arptable

Success.

DES-3200-28:4#
```

ROUTING TABLE COMMANDS

The Routing Table commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create iproute	[default] <ipaddr> {<metric 1-65535>}
delete iproute	[default]
show iproute	{<network_address> static}
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]
create ipv6route	[default] [<ipif_name 12> <ipv6addr> <ipv6addr>] {<metric 1-65535>}
delete ipv6route	[[default] [<ipif_name 12> <ipv6addr> <ipv6addr>] all]
show ipv6 nd	{ipif <ipif_name 12>}
show ipv6route	
config ipv6 nd ns ipif	<ipif name 12> retrans_time <uint 0–4294967295>

Each command is listed, in detail, in the following sections.

create iproute

Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	create iproute [default] <ipaddr> {<metric 1-65535>}
Description	This command is used to create a default static IP route entry to the Switch's IP routing table.
Parameters	<ipaddr> – The gateway IP address for the next hop router. <metric 1-65535> – Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add the default static address 10.48.74.121, with a metric setting of 1, to the routing table:

```
DES-3200-28:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DES-3200-28:4#
```

delete iproute

Purpose	Used to delete a default IP route entry from the Switch's IP routing
----------------	--

delete iproute

	table.
Syntax	delete iproute [default]
Description	This command is used to delete an existing default entry from the Switch's IP routing table.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the default IP route 10.53.13.254:

```
DES-3200-28:4#delete iproute default
Command: delete iproute default

Success.

DES-3200-28:4#
```

show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	show iproute {<network_address> static}
Description	This command is used to display the Switch's current IP routing table.
Parameters	<network_address> – The network IP address. static – Select a static IP route.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DES-3200-28:4#show iproute
Command: show iproute

Routing Table

IP Address/Netmask      Gateway           Interface        Hops    Protocol
-----
0.0.0.0                 10.1.1.254      System           1       Default
10.0.0.0/8              10.48.74.122    System           1       Local

Total Entries: 2

DES-3200-28:4#
```

create ipv6 neighbor_cache ipif

Purpose	Used to add a static neighbor to an IPv6 interface.
Syntax	create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
Description	This command is used to add a static neighbor to an IPv6 interface.

create ipv6 neighbor_cache ipif

Parameters	<ipif_name> – The interface's name. <ipv6addr> – The address of the neighbor. <macaddr> – The MAC address of the neighbor.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a static neighbor cache entry:

```
DES-3200-28:4#create   ipv6   neighbor_cache   ipif   System   3ffc::1
00:01:02:03:04:05
Command: create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05

Success.

DES-3200-28:4#
```

delete ipv6 neighbor_cache ipif

Purpose	Used to delete an IPv6 neighbor from the interface neighbor address cache.
Syntax	delete ipv6 neighbor_cache ipif [<ipif_name 12> all] [<ipv6addr> static dynamic all]
Description	This command is used to delete a neighbor cache entry or static neighbor cache entries from the address cache or all address cache entries on this ipif. Both static and dynamic entry can be deleted.
Parameters	<ipif_name> – The IPv6 interface's name. <ipv6addr> – The address of the neighbor. all – All entries, including static and dynamic entries, will be deleted. static – Delete the static entries. dynamic – Delete the dynamic entries.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a neighbor cache:

```
DES-3200-28:4#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3ffc::1

Success.

DES-3200-28:4#
```

show ipv6 neighbor_cache ipif

Purpose	Used to display the IPv6 neighbor cache.
Syntax	show ipv6 neighbor_cache ipif [<ipif_name 12> all] [ipv6address <ipv6addr> static dynamic all]
Description	This command is used to display the neighbor cache entry for the specified interface. Display a specific entry, all entries, and all static entries.
Parameters	<ipif_name 12> – The interface's name. <ipv6addr> – The address of the entry.

show ipv6 neighbor_cache ipif

	static – The static neighbor cache entry.
	dynamic – The dynamic entries.
Restrictions	None.

Example usage:

To display the neighbors of the interface System:

```
DES-3200-28:4#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

Neighbor                               Linklayer Address      Interface      State
-----
Fe80::20b:6aff:fecf:7ec6             00:0b:6a:cf:7e:c6     System        R

State :
(I) means Incomplete State. (R) means Reachable State.
(S) means Stale State.       (D) means Delay State.
(P) means Probe State.       (T) means Static State.

DES-3200-28:4#
```

create ipv6route

Purpose	Used to create an IPv6 static route.
Syntax	create ipv6route [default] [<ipif_name 12> <ipv6addr>] {<metric 1-65535>}
Description	This command is used to 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.
Parameters	default – Specifies the default route. <ipif_name 12> – Specifies the interface for the route. <ipv6addr> – Specifies the next hop address for this route. <metric 1-65535> – Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add the default static address 10.48.74.121, with a metric setting of 1, to the routing table:

```
DES-3200-28:4#create ipv6route default System 3FFC::1
Command: create ipv6route default System 3FFC::1

Success.

DES-3200-28:4#
```

delete ipv6route

Purpose	Used to delete an IPv6 route.
Syntax	delete ipv6route [[default] [<ipif_name 12> <ipv6addr> all]
Description	This command is used to delete an IPv6 static route. If the next hop is a global address, it is not necessary to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.
Parameters	default – Specifies the default route. <ipv6addr> – Specifies the next hop address for the default route. all – All static created routes will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an IPv6 static route:

```
DES-3200-28:4#delete ipv6route default 3FFC::1
Command: delete ipv6route default 3FFC::1

Success.

DES-3200-28:4#
```

show ipv6 nd

Purpose	Used to display the interface's information.
Syntax	show ipv6 nd {ipif <ipif_name 12>}
Description	This command is used to display the IPv6 ND related configuration.
Parameters	<ipif_name> – The name of the interface.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the interface's information:

```
DES-3200-28:4#show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name      : System
NS Retransmit Time  : 0(ms)

DES-3200-28:4#
```

show ipv6route

Purpose	Used to display IPv6 routes.
Syntax	show ipv6route
Description	This command is used to display IPv6 routes.
Parameters	None.
Restrictions	None.

Example usage:

To display all the IPv6 routes:

```
DES-3200-28:4#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                Protocol: Static Metric: 1
Next Hop   : 3FFC::1             IPIF      : System

Total Entries: 1

DES-3200-28:4#
```

config ipv6 nd ns ipif

Purpose	Used to configure neighbor solicitation related arguments.
Syntax	config ipv6 nd ns ipif <ipif name 12> retrans_time <uint 0-4294967295>
Description	This command is used to configure neighbor solicitation related arguments.
Parameters	<ipif_name> – The name of the interface. retrans_timer – The neighbor solicitation's retransmit timer in milliseconds. This has the same value as ra retrans_time in the config ipv6 nd ra command. If one is configured, the other will change, too.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the IPv6 nd ns interface:

```
DES-3200-28:4#config ipv6 nd ns ipif System retrans_time 10000
Command: config ipv6 nd ns ipif System retrans_time 10000

Success.

DES-3200-28:4#
```

MAC NOTIFICATION COMMANDS

The MAC Notification commands in the Command Line Interface (CLI) are listed, in the following table, along with their appropriate parameters.

Command	Parameters
enable mac_notification	
disable mac_notification	
config mac_notification	{interval <int 1-2147483647> historysize <int 1-500>} (1)
config mac_notification ports	[<portlist> all] [enable disable]
show mac_notification	
show mac_notification ports	{<portlist>}

Each command is listed, in detail, in the following sections.

enable mac_notification

Purpose	Used to enable global MAC address table notification on the Switch.
Syntax	enable mac_notification
Description	This command is used to enable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable MAC notification without changing basic configuration:

```
DES-3200-28:4#enable mac_notification
Command: enable mac_notification

Success.

DES-3200-28:4#
```

disable mac_notification

Purpose	Used to disable global MAC address table notification on the Switch.
Syntax	disable mac_notification
Description	This command is used to disable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable MAC notification without changing basic configuration:


```
DES-3200-28:4#disable mac_notification
Command: disable mac_notification

Success.

DES-3200-28:4#
```

config mac_notification

Purpose	Used to configure MAC address notification.
Syntax	config mac_notification {interval <int 1-2147483647> historysize <int 1-500>} (1)
Description	This command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	interval <int 1-2147483647> – The time in seconds between notifications. The user may choose an interval between 1 and 2147483647 seconds. historysize <1-500> – The maximum number of entries listed in the history log used for notification.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3200-28:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DES-3200-28:4#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	config mac_notification ports [<portlist> all] [enable disable]
Description	This command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	<portlist> – Specifies a port or range of ports to be configured. all – Entering this command will set all ports on the system. [enable disable] – These commands will enable or disable MAC address table notification on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DES-3200-28:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-3200-28:4#
```

show mac_notification

Purpose	Used to display the Switch's MAC address table notification global settings.
Syntax	show mac_notification
Description	This command is used to display the Switch's MAC address table notification global settings.
Parameters	None.
Restrictions	None.

Example usage:

To view the Switch's MAC address table notification global settings:

```
DES-3200-28:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State           : Enabled
Interval        : 1
History Size    : 1

DES-3200-28:4#
```

show mac_notification ports

Purpose	Used to display the Switch's MAC address table notification status settings.
Syntax	show mac_notification ports {<portlist>}
Description	This command is used to display the Switch's MAC address table notification status settings.
Parameters	<portlist> – Specify a port or group of ports to be viewed. Entering this command without the parameter will display the MAC notification table for all ports.
Restrictions	None.

Example usage:

To display all port's MAC address table notification status settings:

```
DES-3200-28:4#show mac_notification ports
```

```
Command: show mac_notification ports
```

```
Port #   MAC Address Table Notification State
```

```
-----
```

1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
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
```

ACCESS AUTHENTICATION CONTROL COMMANDS

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

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

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

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

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

The server verifies the username and password, and the user is granted normal user privileges on the Switch.

The server will not accept the username and password and the user is denied access to the Switch.

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

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

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

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



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

The Access Authentication Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

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

Each command is listed, in detail, in the following sections.

enable authen_policy

Purpose	Used to enable system access authentication policy.
Syntax	enable authen_policy
Description	This command is used to enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the method list and choose a technique for user authentication upon login.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the system access authentication policy:

```
DES-3200-28:4#enable authen_policy
Command: enable authen_policy

Success.

DES-3200-28:4#
```

disable authen_policy

Purpose	Used to disable system access authentication policy.
Syntax	disable authen_policy
Description	This command is used to disable the administrator-defined authentication policy for users trying to access the Switch. When disabled, the Switch will access the local user account database for username and password verification. In addition, the Switch will now accept the local enable password as the authentication for normal users attempting to access administrator level privileges.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the system access authentication policy:

```
DES-3200-28:4#disable authen_policy
Command: disable authen_policy

Success.

DES-3200-28:4#
```

show authen_policy

Purpose	Used to display the system access authentication policy status on the Switch.
Syntax	show authen_policy
Description	This command will show the current status of the access authentication policy on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the system access authentication policy:

```
DES-3200-28:4#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DES-3200-28:4#
```

create authen_login method_list_name

Purpose	Used to create a user defined method list of authentication methods for users logging on to the Switch.
Syntax	create authen_login method_list_name <string 15>
Description	This command is used to create a list for authentication techniques for user login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.
Parameters	<string 15> – Enter an alphanumeric string of up to 15 characters to define the given method list.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the method list “Zira.”:

```
DES-3200-28:4#create authen_login method_list_name Zira
Command: create authen_login method_list_name Zira

Success.

DES-3200-28:4#
```

config authen_login

Purpose	Used to configure a user-defined or default method list of authentication
----------------	---

config authen_login

methods for user login.

Syntax

```
config authen_login [default | method_list_name <string 15>] method
{tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local |
none} (1)
```

Description

This command is used to configure a user-defined or default method list of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like tacacs – xtacacs – local, the Switch will send an authentication request to the first tacacs host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second tacacs host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, xtacacs. If no authentication takes place using the xtacacs list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.

Successful login using any of these methods will give the user a “user” privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the enable admin command, followed by a previously configured password. (See the enable admin part of this section for more detailed information, concerning the enable admin command.)

Parameters

default – The default method list for access authentication, as defined by the user. The user may choose one or a combination of up to four(4) of the following authentication methods:

tacacs – Adding this parameter will require the user to be authenticated using the TACACS protocol from the remote TACACS server hosts of the TACACS server group list.

xtacacs – Adding this parameter will require the user to be authenticated using the XTACACS protocol from the remote XTACACS server hosts of the XTACACS server group list.

tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from the remote TACACS+ server hosts of the TACACS+ server group list.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from the remote RADIUS server hosts of the RADIUS server group list.

server_group <string 15> – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.

local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

none – Adding this parameter will require no authentication to access the Switch.

method_list_name – Enter a previously implemented method list name defined by the user. The user may add one, or a combination of up to four of the following authentication methods to this method list:

tacacs – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.

xtacacs – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.

tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.

config authen_login

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.

server_group <string 15> – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.

local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

none – Adding this parameter will require no authentication to access the Switch.



NOTE: Entering none or local as an authentication protocol will override any other authentication that follows it on a method list or on the default method list.

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To configure the user defined method list “Zira” with authentication methods TACACS, XTACACS and local, in that order.

```
DES-3200-28:4#config authen_login method_list_name Zira method tacacs xtacacs local
Command: config authen_login method_list_name Zira method tacacs xtacacs local

Success.

DES-3200-28:4#
```

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DES-3200-28:4#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

DES-3200-28:4#
```

delete authen_login method_list_name

Purpose

Used to delete a previously configured user defined method list of authentication methods for users logging on to the Switch.

Syntax

delete authen_login method_list_name <string 15>

Description

This command is used to delete a list for authentication methods for user login.

Parameters

<string 15> – Enter an alphanumeric string of up to 15 characters to define the given method list to delete.

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To delete the method list name “Zira”:

```
DES-3200-28:4#delete authen_login method_list_name Zira
Command: delete authen_login method_list_name Zira

Success.

DES-3200-28:4#
```

show authen_login

Purpose	Used to display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	show authen_login [default method_list_name <string 15> all]
Description	This command is used to show a list of authentication methods for user login.
Parameters	<p>default – Entering this parameter will display the default method list for users logging on to the Switch.</p> <p>method_list_name <string 15> – Enter an alphanumeric string of up to 15 characters to define the given method list to view.</p> <p>all – Entering this parameter will display all the authentication login methods currently configured on the Switch.</p> <p>The window will display the following parameters:</p> <p>Method List Name – The name of a previously configured method list name.</p> <p>Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest).</p> <p>Method Name – Defines which security protocols are implemented, per method list name.</p> <p>Comment – Defines the type of Method. User-defined Group refers to server group defined by the user. Built-in Group refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. Keyword refers to authentication using a technique INSTEAD of TACACS / XTACACS / TACACS+ / RADIUS which are local (authentication through the user account on the Switch) and none (no authentication necessary to access any function on the Switch).</p>
Restrictions	None.

Example usage:

To view the authentication login method list named Zira:

```
DES-3200-28:4#show authen_login method_list_name Zira
Command: show authen_login method_list_name Zira

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

DES-3200-28:4#
```

create authen_enable method_list_name

Purpose	Used to create a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	create authen_enable method_list_name <string 15>
Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch

create_authen_enable_method_list_name

	to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight enable method lists can be implemented on the Switch.
Parameters	<string 15> – Enter an alphanumeric string of up to 15 characters to define the given enable method list to create.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a user-defined method list, named “Permit” for promoting user privileges to Administrator privileges:

```
DES-3200-28:4#create_authen_enable_method_list_name Permit
Command: create_authen_enable_method_list_name Permit

Success.

DES-3200-28:4#
```

config_authen_enable

Purpose	Used to configure a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	config_authen_enable [default method_list_name <string 15>] method {tacacs xtacacs tacacs+ radius server_group <string 15> local_enable none} (1)
Description	<p>This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight enable method lists can be implemented simultaneously on the Switch.</p> <p>The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like tacacs – xtacacs – local_enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, xtacacs. If no authentication takes place using the xtacacs list, the local_enable password set in the Switch is used to authenticate the user.</p> <p>Successful authentication using any of these methods will give the user an “Admin” level privilege.</p>
Parameters	<p>default – The default method list for administration rights authentication, as defined by the user. The user may choose one or a combination of up to four of the following authentication methods:</p> <p>tacacs – Adding this parameter will require the user to be authenticated using the TACACS protocol from the remote TACACS server hosts of the TACACS server group list.</p> <p>xtacacs – Adding this parameter will require the user to be authenticated using the XTACACS protocol from the remote XTACACS server hosts of the XTACACS server group list.</p> <p>tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from the remote</p>

config authen_enable

TACACS+ server hosts of the TACACS+ server group list.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from the remote RADIUS server hosts of the RADIUS server group list.

server_group <string 15> – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.

local_enable – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

none – Adding this parameter will require no authentication to access the Switch.

method_list_name – Enter a previously implemented method list name defined by the user (create authen_enable). The user may add one, or a combination of up to four of the following authentication methods to this method list:

tacacs – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.

xtacacs – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.

tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.

server_group <string 15> – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.

local_enable – Adding this parameter will require the user to be authenticated using the local user account database on the Switch. The local enable password of the device can be configured using the “config admin local_password” command.

none – Adding this parameter will require no authentication to access the administration level privileges on the Switch.

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To configure the user defined method list “Permit” with authentication methods TACACS, XTACACS and local, in that order:

```
DES-3200-28:4#config authen_enable method_list_name Zira method tacacs
xtacacs local_enable
Command: config authen_enable method_list_name Zira method tacacs xtacacs
local_enable

Success.

DES-3200-28:4#
```

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DES-3200-28:4#config  authn_enable  default  method  xtacacs  tacacs+
local_enable
Command: config authn_enable default method xtacacs tacacs+ local_enable

Success.

DES-3200-28:4#
```

delete authn_enable method_list_name

Purpose	Used to delete a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	delete authn_enable method_list_name <string 15>
Description	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	<string 15> – Enter an alphanumeric string of up to 15 characters to define the given enable method list to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user-defined method list “Permit”

```
DES-3200-28:4#delete authn_enable method_list_name Permit
Command: delete authn_enable method_list_name Permit

Success.

DES-3200-28:4#
```

show authn_enable

Purpose	Used to display the method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	show authn_enable [default method_list_name <string 15> all]
Description	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	<p>default – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the Switch.</p> <p>method_list_name <string 15> – Enter an alphanumeric string of up to 15 characters to define the given method list the user wishes to view.</p> <p>all – Entering this parameter will display all the authentication login methods currently configured on the Switch.</p> <p>The window will display the following parameters:</p> <p>Method List Name – The name of a previously configured method list name.</p> <p>Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest).</p> <p>Method Name – Defines which security protocols are implemented, per method list name.</p>

show authen_enable

Comment – Defines the type of Method. User-defined Group refers to server groups defined by the user. Built-in Group refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. Keyword refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the local_enable password on the Switch) and none (no authentication necessary to access any function on the Switch).

Restrictions None.

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DES-3200-28:4#show authen_enable all
```

```
Command: show authen_enable all
```

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

```
Total Entries : 2
```

```
DES-3200-28:4#
```

config authen application

Purpose Used to configure various applications on the Switch for authentication using a previously configured method list.

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

Description This command is used to configure Switch configuration applications (console, telnet, ssh, web) for login at the user level and at the administration level (authen_enable) utilizing a previously configured method list.

Parameters

- application – Choose the application to configure. The user may choose one of the following five options to configure.
 - console – Choose this parameter to configure the command line interface login method.
 - telnet – Choose this parameter to configure the telnet login method.
 - ssh – Choose this parameter to configure the Secure Shell login method.
 - http – Choose this parameter to configure the Web interface login method.
 - all – Choose this parameter to configure all applications (console, telnet, ssh, web) login method.
 - login – Use this parameter to configure an application for normal login on the user level, using a previously configured method list.

config authen application

enable – Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list.

default – Use this parameter to configure an application for user authentication using the default method list.

method_list_name <string 15> – Use this parameter to configure an application for user authentication using a previously configured method list. Enter an alphanumeric string of up to 15 characters to define a previously configured method list.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the Web interface:

```
DES-3200-28:4#config authen application http login default
Command: config authen application http login default

Success.

DES-3200-28:4#
```

show authen application

Purpose Used to display authentication methods for the various applications on the Switch.

Syntax show authen application

Description This command is used to display all of the authentication method lists (login, enable administrator privileges) for Switch configuration applications (console, telnet, SSH, Web) currently configured on the Switch.

Parameters None.

Restrictions None.

Example usage:

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

```
DES-3200-28:4#show authen application
Command: show authen application

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

DES-3200-28:4#
```

create authen server_host

Purpose Used to create an authentication server host.

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

create authen server_host

	1-255> retransmit < 1-255>}
Description	This command is used to create an authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	<p>server_host <ipaddr> – The IP address of the remote server host to add.</p> <p>protocol – The protocol used by the server host. The user may choose one of the following:</p> <p>tacacs – Enter this parameter if the server host utilizes the TACACS protocol.</p> <p>xtacacs – Enter this parameter if the server host utilizes the XTACACS protocol.</p> <p>tacacs+ – Enter this parameter if the server host utilizes the TACACS+ protocol.</p> <p>radius – Enter this parameter if the server host utilizes the RADIUS protocol.</p> <p>port <int 1-65535> – Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.</p> <p>key <key_string 254> – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters.</p> <p>timeout <int 1-255> – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.</p> <p>retransmit <int 1-255> – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a TACACS+ authentication server host, with port number 1234, a timeout value of 10 seconds and a retransmit count of 5.

```
DES-3200-28:4#create authen server_host 10.1.1.121 protocol tacacs+ port
1234 timeout 10 retransmit 5
Command: create authen server_host 10.1.1.121 protocol tacacs+ port 1234
timeout 10 retransmit 5

Success.

DES-3200-28:4#
```

config authen server_host

Purpose	Used to configure a user-defined authentication server host.
----------------	--

config authen server_host

Syntax	config authen server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius] {port <int 1-65535> key [<key_string 254> none] timeout <int 1-255> retransmit < 1-255>} (1)
Description	This command is used to configure a user-defined authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	<p>server_host <ipaddr> – The IP address of the remote server host the user wishes to alter.</p> <p>protocol – The protocol used by the server host. The user may choose one of the following:</p> <p>tacacs – Enter this parameter if the server host utilizes the TACACS protocol.</p> <p>xtacacs – Enter this parameter if the server host utilizes the XTACACS protocol.</p> <p>tacacs+ – Enter this parameter if the server host utilizes the TACACS+ protocol.</p> <p>radius – Enter this parameter if the server host utilizes the RADIUS protocol.</p> <p>port <int 1-65535> – Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.</p> <p>key <key_string 254> – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters or choose none.</p> <p>timeout <int 1-255> – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.</p> <p>retransmit <int 1-255> – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond. This field is inoperable for the TACACS+ protocol.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a TACACS+ authentication server host, with port number 4321, a timeout value of 12 seconds and a retransmit count of 4.

```
DES-3200-28:4#config authen server_host 10.1.1.121 protocol tacacs+ port
4321 timeout 12 retransmit 4
Command: config authen server_host 10.1.1.121 protocol tacacs+ port 4321
timeout 12 retransmit 4

Success.

DES-3200-28:4#
```

delete authen server_host

Purpose	Used to delete a user-defined authentication server host.
Syntax	delete authen server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius]
Description	This command is used to delete a user-defined authentication server host previously created on the Switch.
Parameters	<p>server_host <ipaddr> – The IP address of the remote server host to be deleted.</p> <p>protocol – The protocol used by the server host the user wishes to delete. The user may choose one of the following:</p> <p>tacacs – Enter this parameter if the server host utilizes the TACACS protocol.</p> <p>xtacacs – Enter this parameter if the server host utilizes the XTACACS protocol.</p> <p>tacacs+ – Enter this parameter if the server host utilizes the TACACS+ protocol.</p> <p>radius – Enter this parameter if the server host utilizes the RADIUS protocol.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a user-defined TACACS+ authentication server host:

```
DES-3200-28:4#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DES-3200-28:4#
```

show authen server_host

Purpose	Used to view a user-defined authentication server host.
Syntax	show authen server_host
Description	<p>This command is used to view user-defined authentication server hosts previously created on the Switch.</p> <p>The following parameters are displayed:</p> <p>IP Address – The IP address of the authentication server host.</p> <p>Protocol – The protocol used by the server host. Possible results will include TACACS, XTACACS, TACACS+ or RADIUS.</p>

show authen server_host

	Port – The virtual port number on the server host. The default value is 49.
	Timeout – The time in seconds the Switch will wait for the server host to reply to an authentication request.
	Retransmit – The value in the retransmit field denotes how many times the device will resend an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol.
	Key – Authentication key to be shared with a configured TACACS+ server only.
Parameters	None.
Restrictions	None.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DES-3200-28:4#show authen server_host
Command: show authen server_host

IP Address      Protocol      Port  Timeout  Retransmit  Key
-----
10.53.13.94    TACACS       49    5         2           No Use

Total Entries : 1

DES-3200-28:4#
```

create authen server_group

Purpose	Used to create a user-defined authentication server group.
Syntax	create authen server_group <string 15>
Description	This command is used to create an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may add up to eight authentication server hosts to this group using the config authen server_group command.
Parameters	<string 15> – Enter an alphanumeric string of up to 15 characters to define the newly created server group.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the server group “group_1”:

```
DES-3200-28:4#create authen server_group group_1
Command: create authen server_group group_1

Success.

DES-3200-28:4#
```

config authen server_group

Purpose	Used to configure a user-defined authentication server group.
Syntax	config authen server_group [tacacs xtacacs tacacs+ radius <string 15>] [add delete] server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius]
Description	This command is used to configure an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. Up to eight authentication server hosts may be added to any particular group
Parameters	<p>server_group – The user may define the group by protocol groups built into the Switch (TACACS/XTACACS/TACACS+/RADIUS), or by a user-defined group previously created using the create authen server_group command.</p> <p>tacacs – Use this parameter to utilize the built-in TACACS server protocol on the Switch. Only server hosts utilizing the TACACS protocol may be added to this group.</p> <p>xtacacs – Use this parameter to utilize the built-in XTACACS server protocol on the Switch. Only server hosts utilizing the XTACACS protocol may be added to this group.</p> <p>tacacs+ – Use this parameter to utilize the built-in TACACS+ server protocol on the Switch. Only server hosts utilizing the TACACS+ protocol may be added to this group.</p> <p>radius – Use this parameter to utilize the built-in RADIUS server protocol on the Switch. Only server hosts utilizing the RADIUS protocol may be added to this group.</p> <p><string 15> – Enter an alphanumeric string of up to 15 characters to define the previously created server group. This group may add any combination of server hosts to it, regardless of protocol.</p> <p>add/delete – Enter the correct parameter to add or delete a server host from a server group.</p> <p>server_host <ipaddr> – Enter the IP address of the previously configured server host to add or delete.</p> <p>protocol – Enter the protocol utilized by the server host. There are four options:</p> <p>tacacs – Use this parameter to define the protocol if the server host is using the TACACS authentication protocol.</p> <p>xtacacs – Use this parameter to define the protocol if the server host is using the XTACACS authentication protocol.</p> <p>tacacs+ – Use this parameter to define the protocol if the server host is using the TACACS+ authentication protocol.</p> <p>radius – Use this parameter to define the protocol if the server host is using the RADIUS authentication protocol.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add an authentication host to server group “group_1”:

```
DES-3200-28:4# config authn server_group group_1 add server_host
10.1.1.121 protocol tacacs+
Command: config authn server_group group_1 add server_host 10.1.1.121
protocol tacacs+

Success.

DES-3200-28:4#
```

delete authn server_group

Purpose	Used to delete a user-defined authentication server group.
Syntax	delete authn server_group <string 15>
Description	This command is used to delete an authentication server group.
Parameters	<string 15> – Enter an alphanumeric string of up to 15 characters to define the previously created server group to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the server group “group_1”:

```
DES-3200-28:4#delete authn server_group group_1
Command: delete authn server_group group_1

Success.

DES-3200-28:4#
```

show authn server_group

Purpose	Used to view authentication server groups on the Switch.
Syntax	show authn server_group <string 15>
Description	This command is used to display authentication server groups currently configured on the Switch. This command will display the following fields: Group Name – The name of the server group currently configured on the Switch, including built in groups and user defined groups. IP Address – The IP address of the server host. Protocol – The authentication protocol used by the server host.
Parameters	<string 15> – Enter an alphanumeric string of up to 15 characters to define the previously created server group to be viewed. Entering this command without the <string> parameter will display all authentication server groups on the Switch.
Restrictions	None.

Example usage:

To view authentication server groups currently set on the Switch.

```
DES-3200-28:4#show authen server_group
Command: show authen server_group

Group Name      IP Address      Protocol
-----
radius          -----
tacacs          -----
tacacs+         -----
xtacacs         -----

Total Entries : 4

DES-3200-28:4#
```

config authen parameter response_timeout	
Purpose	Used to configure the amount of time the Switch will wait for a user to enter authentication before timing out.
Syntax	config authen parameter response_timeout <int 0-255>
Description	This command is used to set the time the Switch will wait for a response of authentication from the user.
Parameters	response_timeout <int 0-255> – Set the time, in seconds, the Switch will wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. 0 means there won't be a time-out. The default value is 30 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the response timeout for 60 seconds:

```
DES-3200-28:4#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DES-3200-28:4#
```

config authen parameter attempt	
Purpose	Used to configure the maximum number of times the Switch will accept authentication attempts.
Syntax	config authen parameter attempt <int 1-255>
Description	This command is used to configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet users will be disconnected from the Switch.
Parameters	parameter attempt <int 1-255> – Set the maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the maximum number of authentication attempts at 5:

```
DES-3200-28:4#config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DES-3200-28:4#
```

show authen parameter	
Purpose	Used to display the authentication parameters currently configured on the Switch.
Syntax	show authen parameter
Description	<p>This command will display the authentication parameters currently configured on the Switch, including the response timeout and user authentication attempts.</p> <p>This command will display the following fields:</p> <p>Response timeout – The configured time allotted for the Switch to wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface.</p> <p>User attempts – The maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.</p>
Parameters	None.
Restrictions	None.

Example usage:

To view the authentication parameters currently set on the Switch:

```
DES-3200-28:4#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 5

DES-3200-28:4#
```

enable admin	
Purpose	Used to promote user level privileges to administrator level privileges.
Syntax	enable admin
Description	<p>This command is for users who have logged on to the Switch on the normal user level to become promoted to the administrator level. After logging on to the Switch users will have only user level privileges. To gain access to administrator level privileges, the user will enter this command and will have to enter an authentication password. Possible authentication methods for this function include TACACS, XTACACS, TACACS+, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host which has the username “enable”, and a password configured by the administrator that will support the “enable” function. This function becomes inoperable when the authentication policy is disabled.</p>
Parameters	None.

enable admin

Restrictions None.

Example usage:

To enable administrator privileges on the Switch:

```
DES-3200-28:4#enable admin
Password: *****

DES-3200-28:4#
```

config admin local_enable

Purpose	Used to configure the local enable password for administrator level privileges.
Syntax	config admin local_enable
Description	This command is used to configure the locally enabled password for the enable admin command. When a user chooses the “local_enable” method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is set locally on the Switch.
Parameters	<password 15> – After entering this command, the user will be prompted to enter the old password, then a new password in an alphanumeric string of no more than 15 characters, and finally prompted to enter the new password again for confirmation. See the example below.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the password for the “local_enable” authentication method.

```
DES-3200-28:4#config admin local_enable
Command: config admin local_enable

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

DES-3200-28:4#
```


SSH COMMANDS

The steps required to use the Secure Shell (SSH) protocol for secure communication between a remote PC (the SSH Client) and the Switch (the SSH Server), are as follows:

Create a user account with admin-level access using the `create account admin <username> <password>` command. This is identical to creating any other admin-level user account on the Switch, including specifying a password. This password is used to login to the Switch, once secure communication has been established using the SSH protocol.

Configure the user account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the `config ssh authmode` command. There are three choices as to the method SSH will use to authorize the user, and they are `password`, `publickey` and `hostbased`.

Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH Client and the SSH Server.

Finally, enable SSH on the Switch using the `enable ssh` command.

After following the above steps, users can configure an SSH Client on the remote PC and manage the Switch using secure, in-band communication.

The Secure Shell (SSH) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
<code>enable ssh</code>	
<code>disable ssh</code>	
<code>config ssh authmode</code>	[<code>password</code> <code>publickey</code> <code>hostbased</code>] [<code>enable</code> <code>disable</code>]
<code>show ssh authmode</code>	
<code>config ssh server</code>	{ <code>maxsession <int 1-8></code> <code>contimeout <sec 120-600></code> <code>authfail <int 2-20></code> <code>rekey [10min 30min 60min never]</code> } (1)
<code>show ssh server</code>	
<code>config ssh user</code>	<username 15> <code>authmode</code> [<code>hostbased</code> [<code>hostname <domain_name 32></code> <code>hostname_IP <domain_name 32></code> <code><ipaddr></code>] <code>password</code> <code>publickey</code>]
<code>show ssh user authmode</code>	
<code>config ssh algorithm</code>	[<code>3DES</code> <code>AES128</code> <code>AES192</code> <code>AES256</code> <code>arcfour</code> <code>blowfish</code> <code>cast128</code> <code>twofish128</code> <code>twofish192</code> <code>twofish256</code> <code>MD5</code> <code>SHA1</code> <code>RSA</code> <code>DSA</code>] [<code>enable</code> <code>disable</code>]
<code>show ssh algorithm</code>	

Each command is listed, in detail, in the following sections.

enable ssh

Purpose	Used to enable SSH.
Syntax	<code>enable ssh</code>
Description	This command is used to enable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To enable SSH:

```
DES-3200-28:4#enable ssh
```

```
Command: enable ssh
```

```
Success.
```

```
DES-3200-28:4#
```

disable ssh

Purpose	Used to disable SSH.
Syntax	disable ssh
Description	This command is used to disable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To disable SSH:

```
DES-3200-28:4# disable ssh
```

```
Command: disable ssh
```

```
Success.
```

```
DES-3200-28:4#
```

config ssh authmode

Purpose	Used to configure the SSH authentication mode setting.
Syntax	config ssh authmode [password publickey hostbased] [enable disable]
Description	This command is used to configure the SSH authentication mode for users attempting to access the Switch.
Parameters	<p>password – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the Switch.</p> <p>publickey – This parameter may be chosen if the administrator wishes to use a publickey configuration set on a SSH server, for authentication.</p> <p>hostbased – This parameter may be chosen if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed.</p> <p>[enable disable] – This allows users to enable or disable SSH authentication on the Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DES-3200-28:4#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

DES-3200-28:4#
```

show ssh authmode	
Purpose	Used to display the SSH authentication mode setting.
Syntax	show ssh authmode
Description	This command is used to display the current SSH authentication set on the Switch.
Parameters	None.
Restrictions	None.

Example usage:
 To view the current authentication mode set on the Switch:

```
DES-3200-28:4#show ssh authmode
Command: show ssh authmode

The SSH Authmode:
-----
Password   : Enabled
Publickey  : Enabled
Hostbased  : Enabled

DES-3200-28:4#
```

config ssh server	
Purpose	Used to configure the SSH server.
Syntax	config ssh server {maxsession <int 1-8> timeout <sec 120-600> authfail <int 2-20> rekey [10min 30min 60min never]} (1)
Description	This command is used to configure the SSH server.
Parameters	<p>maxsession <int 1-8> – Allows the user to set the number of users that may simultaneously access the Switch. The default setting is 8.</p> <p>timeout <sec 120-600> – Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default is 120 seconds.</p> <p>authfail <int 2-20> – Allows the administrator to set the maximum number of attempts that a user may try to logon utilizing SSH authentication. After the maximum number of attempts is exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login.</p> <p>rekey [10min 30min 60min never] – Sets the time period that the Switch will change the security shell encryptions.</p>

config ssh server

Restrictions Only Administrator-level users can issue this command.

Usage example:

To configure the SSH server:

```
DES-3200-28:4# config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2

Success.

DES-3200-28:4#
```

show ssh server

Purpose	Used to display the SSH server setting.
Syntax	show ssh server
Description	This command is used to display the current SSH server setting.
Parameters	None.
Restrictions	None.

Usage example:

To display the SSH server:

```
DES-3200-28:4# show ssh server
Command: show ssh server

SSH Server Status           : Disabled
SSH Max Session             : 8
Connection Timeout         : 120 (sec)
Authenticate Failed Attempts : 2
Rekey Timeout               : never
Listened Port Number        : 22

DES-3200-28:4#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	config ssh user <username 15> authmode [hostbased [hostname <domain_name 32>] [hostname_IP <domain_name 32> <ipaddr>] password publickey]
Description	This command is used to configure the SSH user authentication method.
Parameters	<p><username 15> – Enter a username of no more than 15 characters to identify the SSH user.</p> <p>authmode – Specifies the authentication mode of the SSH user wishing to log on to the Switch. The administrator may choose between:</p> <ul style="list-style-type: none"> hostbased – This parameter should be chosen if the user wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user.

config ssh user

hostname <domain_name 32> – Enter an alphanumeric string of up to 32 characters identifying the remote SSH user.

hostname_IP <domain_name 32> <ipaddr> – Enter the hostname and the corresponding IP address of the SSH user.

password – This parameter should be chosen to use an administrator defined password for authentication. Upon entry of this command, the Switch will prompt the user for a password, and then to retype the password for confirmation.

publickey – This parameter should be chosen to use the publickey on a SSH server for authentication.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the SSH user:

```
DES-3200-28:4# config ssh user Zira authmode password
Command: config ssh user Zira authmode password

Success.

DES-3200-28:4#
```

show ssh user authmode

Purpose	Used to display the SSH user setting.
Syntax	show ssh user authmode
Description	This command is used to display the current SSH user setting.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the SSH user:

```
DES-3200-28:4#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
Username      AuthMode      HostName      HostIP
-----
Zira          Password
Total Entries : 1

DES-3200-28:4#
```



Note: To configure the SSH user, the administrator must create a user account on the Switch. For information concerning configuring a user account, please see the section of this manual entitled Basic Switch Commands and then the command, create account.

config ssh algorithm

Purpose	Used to configure the SSH algorithm.
Syntax	config ssh algorithm [3DES AES128 AES192 AES256 arcfour blowfish cast128 twofish128 twofish192 twofish256 MD5 SHA1 RSA DSA] [enable disable]
Description	This command is used to configure the desired type of SSH algorithm used for authentication encryption.
Parameters	<p>3DES – This parameter will enable or disable the Triple_Data Encryption Standard encryption algorithm.</p> <p>AES128 – This parameter will enable or disable the Advanced Encryption Standard AES128 encryption algorithm.</p> <p>AES192 – This parameter will enable or disable the Advanced Encryption Standard AES192 encryption algorithm.</p> <p>AES256 – This parameter will enable or disable the Advanced Encryption Standard AES256 encryption algorithm.</p> <p>arcfour – This parameter will enable or disable the Arcfour encryption algorithm.</p> <p>blowfish – This parameter will enable or disable the Blowfish encryption algorithm.</p> <p>cast128 – This parameter will enable or disable the Cast128 encryption algorithm.</p> <p>twofish128 – This parameter will enable or disable the twofish128 encryption algorithm.</p> <p>twofish192 – This parameter will enable or disable the twofish192 encryption algorithm.</p> <p>MD5 – This parameter will enable or disable the MD5 Message Digest encryption algorithm.</p> <p>SHA1 – This parameter will enable or disable the Secure Hash Algorithm encryption.</p> <p>RSA – This parameter will enable or disable the RSA encryption algorithm.</p> <p>DSA – This parameter will enable or disable the Digital Signature Algorithm encryption.</p> <p>[enable disable] – This allows the user to enable or disable algorithms entered in this command, on the Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To configure SSH algorithm:

```
DES-3200-28:4# config ssh algorithm blowfish enable
Command: config ssh algorithm blowfish enable

Success.

DES-3200-28:4#
```

show ssh algorithm

Purpose	Used to display the SSH algorithm setting.
Syntax	show ssh algorithm
Description	This command will display the current SSH algorithm setting status.

show ssh algorithm**Parameters** None.**Restrictions** None.

Usage Example:

To display SSH algorithms currently set on the Switch:

```

DES-3200-28:4#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
-----
3DES           : Enabled
AES128         : Enabled
AES192         : Enabled
AES256         : Enabled
arcfour        : Enabled
blowfish       : Enabled
cast128        : Enabled
twofish128    : Enabled
twofish192    : Enabled
twofish256    : Enabled

Data Integrity Algorithm
-----
MD5            : Enabled
SHA1           : Enabled

Public Key Algorithm
-----
RSA            : Enabled

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

```

SSL COMMANDS

Secure Sockets Layer or SSL is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a ciphersuite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

Key Exchange: The first part of the ciphersuite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE_DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.

Encryption: The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

Stream Ciphers – There are two types of stream ciphers on the Switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES_EDE encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

Hash Algorithm: This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, MD5 (Message Digest 5) and SHA (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

The SSL commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
enable ssl	{ciphersuite {RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5} (1) }
disable ssl	{ciphersuite {RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5} (1) }
config ssl cachetimeout timeout	<value 60-86400>
show ssl	
show ssl certificate	
show ssl cachetimeout	
download ssl certificate	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

Each command is listed, in detail, in the following sections.

enable ssl

Purpose	To enable the SSL function on the Switch.
Syntax	enable ssl {ciphersuite {RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5} (1) }
Description	This command is used to enable SSL on the Switch by implementing any one or combination of listed ciphersuites on the Switch. Entering this command without a parameter will enable the SSL status on the Switch. Enabling SSL will disable the web-manager on the Switch.
Parameters	<p>ciphersuite – A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following:</p> <p>RSA_with_RC4_128_MD5 – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm.</p> <p>RSA_with_3DES_EDE_CBC_SHA – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm.</p> <p>DHE_DSS_with_3DES_EDE_CBC_SHA – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm.</p> <p>RSA_EXPORT_with_RC4_40_MD5 – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.</p> <p>The ciphersuites are enabled by default on the Switch, yet the SSL status is disabled by default. Enabling SSL with a ciphersuite will not enable the SSL status on the Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DES-3200-28:4#enable ssl
Command: enable ssl

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

DES-3200-28:4#
```



NOTE: Enabling SSL on the Switch will enable all ciphersuites. To utilize a particular ciphersuite, the user must eliminate other ciphersuites by using the disable ssl command along with the appropriate ciphersuites.



NOTE: Enabling the SSL function on the Switch will disable the port for the web manager (port 80). To log on to the web based manager, the entry of the URL must begin with https://. (ex. https://10.90.90.90).

disable ssl

Purpose	To disable the SSL function on the Switch.
Syntax	disable ssl {ciphersuite {RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5} (1) }
Description	This command is used to disable SSL on the Switch and can be used to disable any one or combination of listed ciphersuites on the Switch.
Parameters	<p>ciphersuite - A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following:</p> <ul style="list-style-type: none"> RSA_with_RC4_128_MD5 – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. RSA_with_3DES_EDE_CBC_SHA – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. DHE_DSS_with_3DES_EDE_CBC_SHA – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. RSA_EXPORT_with_RC4_40_MD5 – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DES-3200-28:4#disable ssl
Command: disable ssl

Success.

DES-3200-28:4#
```

To disable ciphersuite RSA_EXPORT_with_RC4_40_MD5 only:

```
DES-3200-28:4#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5

Success.

DES-3200-28:4#
```

config ssl cachetimeout timeout

Purpose	Used to configure the SSL cache timeout.
Syntax	config ssl cachetimeout timeout <value 60-86400>
Description	This command is used to set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process.
Parameters	timeout <value 60-86400> – Enter a timeout value between 60 and 86400 seconds to specify the total time an SSL key exchange ID stays valid before the SSL module will require a new, full SSL negotiation for connection. The default cache timeout is 600 seconds
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the SSL cachetimeout for 7200 seconds:

```
DES-3200-28:4#config ssl cachetimeout timeout 7200
Command: config ssl cachetimeout timeout 7200

Success.

DES-3200-28:4#
```

show ssl cachetimeout

Purpose	Used to show the SSL cache timeout.
Syntax	show ssl cachetimeout
Description	This command is used to view the SSL cache timeout currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL cache timeout on the Switch:

```
DES-3200-28:4#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DES-3200-28:4#
```

show ssl

Purpose	Used to view the SSL status and the certificate file status on the Switch.
Syntax	show ssl
Description	This command is used to view the SSL status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DES-3200-28:4#show ssl
Command: show ssl

SSL Status                               Disabled
RSA_WITH_RC4_128_MD5                     0x0004 Enabled
RSA_WITH_3DES_EDE_CBC_SHA                 0x000A Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA            0x0013 Enabled
RSA_EXPORT_WITH_RC4_40_MD5               0x0003 Enabled

DES-3200-28:4#
```

show ssl certificate	
Purpose	Used to view the SSL certificate file status on the Switch.
Syntax	show ssl certificate
Description	This command is used to view the SSL certificate file information currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view certificate file information on the Switch:

```
DES-3200-28:4# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DES-3200-28:4#
```

download ssl certificate	
Purpose	Used to download a certificate file for the SSL function on the Switch.
Syntax	download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
Description	This command is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions.
Parameters	<ipaddr> – Enter the IP address of the TFTP server. certfilename <path_filename 64> – Enter the path and the filename of the certificate file users wish to download. keyfilename <path_filename 64> – Enter the path and the filename of the key exchange file users wish to download.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download a certificate file and key file to the Switch:

```
DES-3200-28:4#download ssl certificate 10.53.13.94 certfilename
c:/cert.der keyfilename c:/pkey.der
Command: download ssl certificate 10.53.13.94 certfilename c:/cert.der
keyfilename c:/pkey.der

Certificate Loaded Successfully!

DES-3200-28:4#
```

D-LINK SINGLE IP MANAGEMENT COMMANDS

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

SIM is an optional feature on the Switch and can easily be enabled or disabled. SIM grouping has no effect on the normal operation of the Switch in the user's network.

There are three classifications for switches using SIM. The Commander Switch(CS), which is the master switch of the group, Member Switch(MS), which is a switch that is recognized by the CS a member of a SIM group, and a Candidate Switch(CaS), which is a switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

A SIM group can only have one Commander Switch(CS).

All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

A SIM group accepts one Commander Switch (numbered 0) and up to 32 switches (numbered 0-31).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.

SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that is more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The Switch may take on three different roles:

Commander Switch (CS) – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:

It has an IP Address.

It is not a Commander Switch or Member Switch of another Single IP group.

It is connected to the Member Switches through its management VLAN.

Member Switch (MS) – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:

It is not a CS or MS of another IP group.

It is connected to the CS through the CS management VLAN.

Candidate Switch (CaS) – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group through an automatic function of the Switch, or by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

It is not a CS or MS of another Single IP group.

It is connected to the CS through the CS management VLAN.

The following rules also apply to the above roles:

Each device begins in the Candidate state.

CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus the CS cannot directly be converted to a MS.

The user can manually configure a CS to become a CaS.

A MS can become a CaS by:

Being configured as a CaS through the CS.

If report packets from the CS to the MS time out.

The user can manually configure a CaS to become a CS

The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional Switches may join the group by either an automatic method or by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send back to the administrator.

When a CS becomes a MS, it automatically becomes a member of the first SNMP community (includes read/write and read only) to which the CS belongs.

The Upgrade to v1.6

To better improve SIM management, the Switch has been upgraded to version 1.6 in this release. Many improvements have been made, including:

The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintain packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches. There are some instances where pre-saved MS switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

This version will support multiple switch upload and downloads for firmware, configuration files and log files, as follows:

Firmware – The switch now supports multiple MS firmware downloads from a TFTP server.

Configuration Files – This switch now supports multiple downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server..

Log – The switch now supports uploading multiple MS log files to a TFTP server.



NOTE: For more details regarding improvements made in SIMv1.6, please refer to the White Paper located on the D-Link website.

The D-Link Single IP Management commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
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]

Each command is listed, in detail, in the following sections:

enable sim

Purpose	Used to enable Single IP Management (SIM) on the Switch.
Syntax	enable sim
Description	This command is used to enable SIM globally on the Switch. SIM features and functions will not function properly unless this function is enabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SIM on the Switch:

```
DES-3200-28:4#enable sim
Command: enable sim

Success.

DES-3200-28:4#
```

disable sim

Purpose	Used to disable Single IP Management (SIM) on the Switch.
Syntax	disable sim
Description	This command is used to disable SIM globally on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SIM on the Switch:

```
DES-3200-28:4#disable sim
Command: disable sim

Success.

DES-3200-28:4#
```


show sim

Purpose	Used to view the current information regarding the SIM group on the Switch.
Syntax	show sim {[candidates {<candidate_id 1-100>} members {<member_id 1-32>} group {commander_mac <macaddr>} neighbor}}
Description	<p>This command is used to display the current information regarding the SIM group on the Switch, including the following:</p> <p>SIM Version – Displays the current Single IP Management version on the Switch.</p> <p>Firmware Version – Displays the current Firmware version on the Switch.</p> <p>Device Name – Displays the user-defined device name on the Switch.</p> <p>MAC Address – Displays the MAC Address of the Switch.</p> <p>Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3).</p> <p>Platform – Switch Description including name and model number.</p> <p>SIM State – Displays the current Single IP Management State of the Switch, whether it be enabled or disabled.</p> <p>Role State – Displays the current role the Switch is taking, including Commander, Member or Candidate. A Stand-alone switch will always have the commander role.</p> <p>Discovery Interval – Time in seconds the Switch will send discovery packets out over the network.</p> <p>Hold time – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.</p>
Parameters	<p>candidates {<candidate_id 1-100>} – Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's ID number, listed from 1 to 100.</p> <p>members {<member_id 1-32>} – Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's id number, listed from 1 to 32.</p> <p>group {commander_mac <macaddr>} – Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group.</p> <p>neighbor – Entering this parameter will display neighboring devices of the Switch. A SIM neighbor is defined as a switch that is physically connected to the Switch but is not part of the SIM group. This screen will produce the following results:</p> <p>Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located.</p> <p>MAC Address – Displays the MAC Address of the neighbor switch.</p> <p>Role – Displays the role(CS, CaS, MS) of the neighbor switch.</p>
Restrictions	None.

Example usage:

To show the SIM information in detail:

```
DES-3200-28:4#show sim
Command: show sim

SIM Version      : VER-1.6.07
Firmware Version : 1.28.005
Device Name      :
MAC Address      : 00-63-32-28-01-01
Capabilities     : L2
Platform        : DES-3200-28 L2 Switch
SIM State       : Disabled
Role State      : Candidate
Discovery Interval : 30 sec
Holdtime        : 100 sec

DES-3200-28:4#
```

To show the candidate information in summary:

```
DES-3200-28:4#show sim candidates
Command: show sim candidates

ID   MAC Address           Platform /
    Capability           Hold   Firmware   Device Name
    Time                Version
-----
1   00-01-02-03-04-00   DES-3200-28 L2 Switch  40    1.28.005   The Man
2   00-55-55-00-55-00   DES-3200-28 L2 Switch  140   1.28.005   default master

Total Entries: 2

DES-3200-28:4#
```

To show the member information in summary:

```
DES-3200-28:4#show sim members
Command: show sim members

ID   MAC Address           Platform /
    Capability           Hold   Firmware   Device Name
    Time                Version
-----
1   00-01-02-03-04-00   DES-3200-28 L2 Switch  40    2.00.B23   The Man
2   00-55-55-00-55-00   DES-3200-28 L2 Switch  140   2.00.B23   default master

Total Entries: 2

DES-3200-28:4#
```

To show other groups information in summary:

```
DES-3200-28:4#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address          Platform /
   MAC Address          Capability
   Hold Time           Firmware Version   Device Name
-----
*1  00-01-02-03-04-00    DES-3200-28 L2 Switch  40      1.28.005   Gallinari
 2  00-55-55-00-55-00    DES-3200-28 L2 Switch  140     1.28.005   default master

SIM Group Name : SIM2

ID  MAC Address          Platform /
   MAC Address          Capability
   Hold Time           Firmware Version   Device Nam
-----
*1  00-44-11-23-04-00    DES-3200-28 L2 Switch  40      1.28.005   Neo
 2  00-22-22-00-55-00    DES-3200-28 L2 Switch  140     1.28.005   default master

DES-3200-28:4#
```

To view SIM neighbors:

```
DES-3200-28:4#show sim neighbor
Command: show sim neighbor

Neighbor Info Table

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

Total Entries: 3

DES-3200-28:4#
```

reconfig	
Purpose	Used to connect to a member switch, through the commander switch, using Telnet.
Syntax	reconfig [member_id <value 1-32> exit]
Description	This command is used to reconnect to a member switch using Telnet and to exit from managing the member switch and return to managing the commander switch.
Parameters	<p>member_id <value 1-32> – Select the ID number of the member switch to configure.</p> <p>exit – This command is used to exit from managing the member switch and will return to managing the commander switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To connect to the MS, with member ID 2, through the CS, using the command line interface:

```
DES-3200-28:4#reconfig member_id 2
Command: reconfig member_id 2

DES-3200-28:4#
```

config sim_group	
Purpose	Used to add candidates and delete members from the SIM group.
Syntax	config sim_group [add <candidate_id 1-100> {<password>} delete <member_id 1-32>]
Description	This command is used to add candidates and delete members from the SIM group by ID number.
Parameters	<p>add <candidate_id 1-100> <password> – Use this parameter to change a candidate switch (CaS) to a member switch (MS) of a SIM group. The CaS may be defined by its ID number and a password (if necessary).</p> <p>delete <member_id 1-32> – Use this parameter to delete a member switch of a SIM group. The member switch should be defined by ID number.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a member:

```
DES-3200-28:4#config sim_group add 1
Command: config sim_group add 1

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

Success.

DES-3200-28:4#
```

To delete a member:

```
DES-3200-28:4# config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!

SIM Config Success !!!

Success.

DES-3200-28:4#
```

config sim	
Purpose	Used to configure role parameters for the SIM protocol on the Switch.
Syntax	config sim [[commander {group_name <groupname 64>} candidate] dp_interval <sec 30-90> hold_time <sec 100-255>]
Description	This command is used to configure parameters of switches of the SIM.
Parameters	commander – Use this parameter to configure a commander switch (CS). candidate – Used to change the role to a CaS (candidate). dp_interval <30-90> – The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to the CS will include information about other switches connected to it. (Ex. MS, CaS). The user may set the dp_interval from 30 to 90 seconds. hold time <100-255> – Using this parameter, the user may set the time, in seconds, the Switch will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 255 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To change the time interval of the discovery protocol:

```
DES-3200-28:4# config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DES-3200-28:4#
```

To change the hold time:

```
DES-3200-28:4# config sim hold_time 120
Command: config sim hold_time 120

Success.

DES-3200-28:4#
```

To transfer the Switch to be a CaS (candidate):

```
DES-3200-28:4# config sim candidate
Command: config sim candidate

Success.

DES-3200-28:4#
```

To transfer the Switch to be a CS (commander):

```
DES-3200-28:4# config sim commander
Command: config sim commander

Success.

DES-3200-28:4#
```

To update the name of a group:

```
DES-3200-28:4# config sim commander group_name Zira
Command: config sim commander group_name Zira

Success.

DES-3200-28:4#
```

download sim

Purpose	Used to download firmware or configuration file to an indicated device.
Syntax	download sim_ms [firmware_from_tftp configuration_from_tftp] <ipaddr> <path_filename> [members <mslist 1-32> all]
Description	This command is used to download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	<p>firmware – Specify this parameter to download firmware to members of a SIM group.</p> <p>configuration – Specify this parameter to download a switch configuration to members of a SIM group.</p> <p><ipaddr> – Enter the IP address of the TFTP server.</p> <p><path_filename> – Enter the path and the filename of the firmware or configuration on the TFTP server.</p> <p>members – Enter this parameter to specify the members to which the user prefers to download firmware or switch configuration files. The user may specify a member or members by adding one of the following:</p> <p><mslist> – Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration.</p> <p>all – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download firmware:

```
DES-3200-28:4#download sim_ms firmware_from_tftp 10.53.13.94 c:/des3200.had
all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/des3200.had all

This device is updating firmware. Please wait several minutes...

Download Status :

ID      MAC Address      Result
---      -
1       00-36-28-10-35-00  Success

DES-3200-28:4#
```

To download configuration files:

```
DES-3200-28:4#download      sim_ms      configuration_from_tftp    10.53.13.94
c:/des3200.txt all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/des3200.txt all

This device is updating configuration. Please wait several minutes...

Download Status :
```

ID	MAC Address	Result
1	00-01-02-03-04-00	Success
2	00-07-06-05-04-03	Success
3	00-07-06-05-04-03	Success

```
DES-3200-28:4#
```

upload sim_ms

Purpose	User to upload a configuration file to a TFTP server from a specified member of a SIM group.
Syntax	upload sim_ms [configuration_to_tftp log_to_tftp] <ipaddr> <path_filename> [members <mslist> all]
Description	This command is used to upload a configuration file or log file to a TFTP server from a specified member of a SIM group.
Parameters	<p><ipaddr> – Enter the IP address of the TFTP server to which to upload a configuration file or a log file.</p> <p><path_filename> – Enter a user-defined path and file name on the TFTP server to which to upload configuration files or log files.</p> <p><mslist> – Enter this parameter to specify the member to which to upload a switch configuration file. The user may specify a member or members by adding the ID number of the specified member.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DES-3200-28:4#upload      sim_ms      configuration_to_tftp      10.55.47.1
D:\configuration.txt members 1
Command: upload sim_ms configuration 10.55.47.1 D:\configuration.txt members 1

This device is upload configuration. Please wait several minutes ...

Upload Status :

ID   MAC Address           Result
---  -
1    00-A1-51-34-26-00    Success

DES-3200-28:4#
```

SMTP COMMANDS

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered using the commands below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events and enhancing security by recording questionable events occurring on the Switch.

The Switch plays four important roles as a client in the functioning of SMTP:

The server and server virtual port must be correctly configured for this function to work properly. This is accomplished in the `config smtp` command by properly configuring the `server` and `server_port` parameters.

Mail recipients must be configured on the Switch. This information is sent to the server which then processes the information and then e-mails Switch information to these recipients. Up to 8 e-mail recipients can be configured on the Switch using the `config smtp` command by configuring the `add mail_receiver` and `delete mail_receiver` parameters.

The administrator can configure the source mail address from which messages are delivered to configured recipients. This can offer more information to the administrator about Switch functions and problems. The personal e-mail can be configured using the `config smtp` command and setting the `self_mail_addr` parameter.

The Switch can be configured to send out test mail to first ensure that the recipient will receive e-mails from the SMTP server regarding the Switch. To configure this test mail, the SMTP function must first be enabled using the `enable smtp` command and then by entering the `smtp send_testmsg` command. All recipients configured for SMTP will receive a sample test message from the SMTP server, ensuring the reliability of this function.

THE SWITCH WILL SEND OUT E-MAIL TO RECIPIENTS WHEN ONE OR MORE OF THE FOLLOWING EVENTS OCCUR:

When a cold start or a warm start occurs on the Switch.

When a port enters a link down status.

When a port enters a link up status.

When SNMP authentication has been denied by the Switch.

When a switch configuration entry has been saved to the NVRAM by the Switch.

When an abnormality occurs on TFTP during a firmware download event. This includes invalid-file, file-not-found, complete and time-out messages from the TFTP server.

When a system reset occurs on the Switch.

Information within the e-mail from the SMTP server regarding switch events includes:

The source device model name and IP address.

A timestamp denoting the identity of the SMTP server and the client that sent the message, as well as the time and date of the message received from the Switch. Messages that have been relayed will have timestamps for each relay.

The event that occurred on the Switch, prompting the e-mail message to be sent.

When an event is processed by a user, such as save or firmware upgrade, the IP address, MAC address and User Name of the user completing the task will be sent along with the system message of the event occurred.

When the same event occurs more than once, the second mail message and every repeating mail message following will have the system's error message placed in the subject line of the mail message.

The following details events occurring during the Delivery Process.

Urgent mail will have high priority and be immediately dispatched to recipients while normal mail will be placed in a queue for future transmission.

The maximum number of untransmitted mail messages placed in the queue cannot exceed 30 messages. Any new messages will be discarded if the queue is full.

If the initial message sent to a mail recipient is not delivered, it will be placed in the waiting queue until its place in the queue has been reached, and then another attempt to transmit the message is made.

The maximum attempts for delivering mail to recipients is three. Mail message delivery attempts will be tried every five minutes until the maximum number of attempts is reached. Once reached and the message has not been successfully delivered, the message will be dropped and not received by the mail recipient.

If the Switch shuts down or reboots, mail messages in the waiting queue will be lost.

The SMTP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
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	

Each command is listed, in detail, in the following sections:

enable smtp	
Purpose	Used to enable the Switch as a SMTP client.
Syntax	enable smtp
Description	This command, in conjunction with the disable smtp command will enable and disable the Switch as a SMTP client without changing configurations.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SMTP on the Switch:

```
DES-3200-28:4#enable smtp
Command: enable smtp

Success.

DES-3200-28:4#
```

disable smtp	
Purpose	Used to disable the Switch as a SMTP client.
Syntax	disable smtp
Description	This command, in conjunction with the enable smtp command will enable and disable the Switch as a SMTP client without changing configurations.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SMTP on the Switch:

```
DES-3200-28:4#disable smtp
```

```
Command: disable smtp
```

```
Success.
```

```
DES-3200-28:4#
```

config smtp

Purpose	Used to configure necessary information in setting up the Switch as an SMTP client.
Syntax	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)
Description	This command is used to set the necessary parameters to configure the SMTP server and mail recipients. This command must be completely configured properly for the SMTP function of the switch to correctly operate.
Parameters	<p>server <ipaddr> – Enter the IP address of the SMTP server on a remote device.</p> <p>server_port <tcp_port_number 1-65535> – Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is 25.</p> <p>self_mail_addr <mail addr 64> – Enter the e-mail address from which mail messages will be sent. This address will be the from address on the e-mail message sent to a recipient. Only one self mail address can be configured for this Switch. This string can be no more than 64 alphanumeric characters.</p> <p>add mail_receiver <mail_addr 64> – Choose this parameter to add mail recipients to receive e-mail messages from the Switch. Up to eight e-mail addresses can be added per Switch.</p> <p>delete mail_receiver <index 1-8> – Choose this parameter to delete mail recipients from the configured list.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the SMTP settings:

```
DES-3200-28:4#config smtp server 166.99.66.33 server_port 25 add mail_receiver ctsnow@axum.com
```

```
Command: config smtp server 166.99.66.33 server_port 25 add mail_receiver ctsnow@axum.com
```

```
Success.
```

```
DES-3200-28:4#
```

show smtp	
Purpose	Used to view configured parameters for the SMTP function on the Switch.
Syntax	show smtp
Description	This command is used to display parameters configured for SMTP on the Switch, including server information, mail recipients and the current running status of SMTP on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SMTP parameters currently configured on the Switch:

```
DES-3200-28:4#show smtp
Command: show smtp

smtp status: Enabled
smtp server address : 166.99.66.33
smtp server port : 25
self mail address: smtp@30XX.dev

Index                Mail Receiver Address
-----
1                    ctsnow@axum.com
2                    clyde@knicks.com
3                    administrator@dlink.com
4                    dgallinari@nba.com
5
6
7
8

DES-3200-28:4#
```

smtp send_testmsg	
Purpose	Used to send a test message to mail recipients configured on the Switch.
Syntax	smtp send_testmsg
Description	This command is used to send test messages to all mail recipients configured on the Switch, thus testing the configurations set and the reliability of the SMTP server.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To send a test mail message to all configured mail recipients:

```
DES-3200-28:4# smtp send_testmsg
Command: smtp send_testmsg

Subject: This is a SMTP test.
Content: Hello everybody!!

Sending mail, please wait...

Success.


DES-3200-28:4#
```

CABLE DIAGNOSTICS COMMANDS

The Cable Diagnostics commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
cable_diag ports	[<portlist> all]

Each command is listed, in detail, in the following sections.

cable_diag ports	
Purpose	Used to test the copper cable. If there is an error on the cable, it can determine the type of error and the position where the error occurred.
Syntax	cable_diag ports [<portlist> all]
Description	<p>For FE port, two pairs of cable will be diagnosed. The type of cable error can be open and short. Open means that the cable in the error pair does not have a connection at the specified position. Short means that the cables in the error pair has a short problem at the specified position. 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. When a port is in link-down status, the link-down may be caused by many factors. When the port has a normal cable connection, but the remote partner is powered off, the cable diagnostics feature can still diagnose the health of the cable as if the remote partner is powered on.</p> <p>When the port does not have any cable connection, the result of the test will indicate no cable. The test will detect the type of error and the position where the error occurs. Note that this test will consume a low number of packets. Since this test is for copper cables, ports with fiber cables will be skipped from the test.</p> <div style="display: flex; align-items: center;">  <div> <p>Note: If the Link Status field for an interface displays "Link Up", the value displayed in the Cable Length field may not be accurate for the interface.</p> </div> </div>
Parameters	<p><portlist> – Specifies a range of ports to be tested.</p> <p>all – All ports</p>
Restrictions	None.

Example usage:

To test the cable on ports 25 to 28:

```
DES-3200-28:4#cable_diag ports 25-28
```

```
Command: cable_diag ports 25-28
```

```
Perform Cable Diagnostics ...
```

Port	Type	Link Status	Test Result	Cable Length (M)
25	GE	Link Up	OK	3
26	GE	Link Down	No Cable	-
27	GE	Link Down	No Cable	-
28	GE	Link Down	No Cable	-

```
DES-3200-28:4#
```


DHCP LOCAL RELAY COMMANDS

The DHCP Local Relay commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config dhcp_local _relay	vlan[<vlan_name 32> vlanid <vidlist>] state [enable disable]
enable dhcp_local _relay	
disable dhcp_local _relay	
show dhcp_local _relay	

Each command is listed, in detail, in the following sections.

config dhcp_local_relay vlan

Purpose	Used to enable or disable the DHCP local relay function for a specified VLAN.
Syntax	config dhcp_local_relay vlan [<vlan_name 32> vlanid <vidlist>] state [enable disable]
Description	This command is used to enable or disable the DHCP local relay function for a specified VLAN. When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed in broadcast way without change of the source MAC address and gateway address. DHCP option 82 will be automatically added.
Parameters	<p><vlan_name 32> – The name of the VLAN to be enabled DHCP local relay.</p> <p><vidlist> – Specifies a range of VLAN IDs to be configured.</p> <p>state – Enable or disable DHCP local relay for specified vlan.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable DHCP local relay for the default VLAN:

```
DES-3200-28:4#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DES-3200-28:4#
```

enable dhcp_local_relay

Purpose	Used to enable the DHCP local relay function on the Switch.
Syntax	enable dhcp_local_relay
Description	This command is used to globally enable the DHCP local relay function on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the DHCP local relay function:

```
DES-3200-28:4#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DES-3200-28:4#
```

disable dhcp_local_relay

Purpose	Used to disable the DHCP local relay function on the Switch.
Syntax	disable dhcp_local_relay
Description	This command is used to globally disable the DHCP local relay function on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the DHCP local relay function:

```
DES-3200-28:4#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DES-3200-28:4#
```

show dhcp_local_relay

Purpose	Used to display the current DHCP local relay configuration.
Syntax	show dhcp_local_relay
Description	This command is used to display the current DHCP local relay configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP local relay function:

```
DES-3200-28:4# show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status      : Disabled
DHCP/BOOTP Local Relay VLAN List  : 1,3-4

DES-3200-28:4#
```

GRATUITOUS ARP COMMANDS

The Gratuitous ARP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config gratuitous_arp send ipif_status_up	[enable disable]
config gratuitous_arp send dup_ip_detected	[enable disable]
config gratuitous_arp learning	[enable disable]
enable gratuitous_arp	{ipif <ipif_name 12>} {trap log} (1)
disable gratuitous_arp	{ipif <ipif_name 12>} {trap log} (1)
config gratuitous_arp send periodically ipif	<ipif_name 12> interval <value 0-65535>
show gratuitous_arp	{ipif <ipif_name 12>}

Each command is listed, in detail, in the following sections.

config gratuitous_arp send ipif_status_up

Purpose	Used to enable or disable the sending of gratuitous ARP requests while the IP interface status is up.
Syntax	config gratuitous_arp send ipif_status_up [enable disable]
Description	The command is used to enable or disable the sending of gratuitous ARP request packets while the IPIF interface is 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.
Parameters	<p>enable – Enable the sending of gratuitous ARP when the IPIF status is up.</p> <p>disable – Disable the sending of gratuitous ARP when the IPIF status is up.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable a gratuitous ARP request:

```
DES-3200-28:4#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DES-3200-28:4#
```

config gratuitous_arp send duplicate_ip_detected

Purpose	Used to enable or disable the sending of gratuitous ARP requests while duplicate IP addresses are detected
Syntax	config gratuitous_arp send duplicate_ip_detected [enable disable]
Description	The command is used to enable or disable the sending of gratuitous ARP request packets while duplicate IPs are detected. By default, the state is enabled.
Parameters	enable – Enable the sending of gratuitous ARP when a duplicate IP is detected. disable – Disable the sending of gratuitous ARP when a duplicate IP is detected.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable gratuitous ARP request when a duplicate IP is detected:

```
DES-3200-28:4#config gratuitous_arp send duplicate_ip_detected enable
Command: config gratuitous_arp send duplicate_ip_detected enable

Success.

DES-3200-28:4#
```

config gratuitous_arp learning

Purpose	Used to enable or disable the learning of ARP entries in ARP cache based on the received gratuitous ARP packets.
Syntax	config gratuitous_arp learning [enable disable]
Description	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 or disable the learning of ARP entries 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 gratuitous ARP learning, the system will not learn new entries but only do the update on the ARP table based on the received gratuitous ARP packet. By default, the state is enabled.
Parameters	enable – Enable the learning of ARP entries based on received gratuitous ARP packets. disable – Disable the learning of ARP entries based on received gratuitous ARP packets.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable learning of ARP entries based on the received gratuitous ARP packets:

```
DES-3200-28:4# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DES-3200-28:4#
```

config gratuitous_arp_send periodically

Purpose	Used to configure the interval for periodical sending of gratuitous ARP request packets.
Syntax	config gratuitous_arp_send periodically ipif <ipif_name 12> interval <value 0-65535>
Description	This command is used to configure the interval for periodical sending of gratuitous ARP request packets. By default, the interval is 0.
Parameters	<ipif_name 12> – The IP interface name of the Switch. <value 0-65535> – Periodically send gratuitous ARP interval time in seconds. 0- means it will not send gratuitous ARP periodically.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure gratuitous ARP intervals for the IPIF System:

```
DES-3200-28:4#config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DES-3200-28:4#
```

enable gratuitous_arp

Purpose	Used to enable the gratuitous ARP trap and log.
Syntax	enable gratuitous_arp {ipif <ipif_name 12>} {trap log} (1)
Description	The command is used to enable gratuitous ARP trap and log states. The Switch can trap and log the IP conflict event to inform the administrator. By default, the trap is disabled and event log is enabled.
Parameters	<ipif_name 12> – IP interface name of the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the System's interface gratuitous ARP log and trap:

```
DES-3200-28:4#enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

DES-3200-28:4#
```

disable gratuitous_arp

Purpose	Used to disable the gratuitous ARP trap and log.
Syntax	disable gratuitous_arp {ipif <ipif_name 12>} {trap log} (1)
Description	The command is used to disable the gratuitous ARP trap and log states. The Switch can trap and log the IP conflict event to inform the administrator. By default, the trap is disabled and event log is enabled.
Parameters	<ipif_name 12> – IP interface name of the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the System's interface gratuitous ARP log and trap:

```
DES-3200-28:4#disable gratuitous_arp ipif system trap log
Command: disable gratuitous_arp ipif system trap log

Success.

DES-3200-28:4#
```

show gratuitous_arp

Purpose	Used to display the gratuitous ARP configuration.
Syntax	show gratuitous_arp {ipif <ipif_name 12>}
Description	This command is used to display the gratuitous ARP configuration.
Parameters	<ipif_name 12> – IP interface name of the Switch.
Restrictions	None.

Example usage:

To display gratuitous ARP log and trap states:

```
DES-3200-28:4# show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF status up          : Enabled
Send on Duplicate_IP_Detected  : Disabled
Gratuitous ARP Learning        : Enabled

IP Interface Name : System
Gratuitous ARP Trap          : Disabled
Gratuitous ARP Log          : Enabled
Gratuitous ARP Periodical Send Interval : 5

Total Entries : 1

DES-3200-28:4#
```

VLAN TRUNKING COMMANDS

The VLAN Trunking commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable vlan_trunk	
disable vlan_trunk	
config vlan_trunk ports	[<portlist> all] state [enable disable]
show vlan_trunk	

Each command is listed, in detail, in the following sections.

enable vlan_trunk

Purpose	Used to enable the VLAN trunk function.
Syntax	enable vlan_trunk
Description	When the VLAN trunk function is enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the VLAN Trunk:

```
DES-3200-28:4#enable vlan_trunk
Command: enable vlan_trunk

Success.

DES-3200-28:4#
```

disable vlan_trunk

Purpose	Used to disable the VLAN trunk function.
Syntax	disable vlan_trunk
Description	This command is used to disable the VLAN trunk function.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the VLAN Trunk:

```
DES-3200-28:4#disable vlan_trunk
Command: disable vlan_trunk

Success.

DES-3200-28:4#
```

config vlan_trunk

Purpose	Used to configure a port as a VLAN trunk port.
Syntax	config vlan_trunk ports [<portlist> all] state [enable disable]
Description	<p>This command is used to configure a port as a VLAN trunk port. By default, none of the ports on the Switch are VLAN trunk ports. 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.</p> <p>If the command is applied to link aggregation member port excluding the master, the command will be rejected.</p> <p>The ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as VLAN trunk ports, they are allowed to form an aggregated link.</p> <p>For a VLAN trunk port, the VLANs on which the packets can be by passed will not be advertised by GVRP on that particular port. However, since the traffic on these VLANs are forwarded, this vlan trunk port should participate the MSTP instances corresponding to these VLAN.</p>
Parameters	<p><portlist> – Specifies the list of ports to be configured.</p> <p>enable – Specifies that the port is a VLAN trunk port.</p> <p>disable – Specifies that the port is not a VLAN trunk port.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a VLAN Trunk port:

```
DES-3200-28:4#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DES-3200-28:4#
```

To configure a VLAN Trunk port if Port 6 is LA-1 member port; port 7 is LA-2 master port.

```
DES-3200-28:4# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Can not operate the member ports of any trunk.

DES-3200-28:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DES-3200-28:4# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Can not operate the member ports of any trunk.

DES-3200-28:4#
```


To configure a VLAN Trunk port if Port 6 is LA-1 member port, port 7 is LA-1 master port.

```
DES-3200-28:4# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DES-3200-28:4#
```

To configure a VLAN Trunk port if Port 6,7 have the same VLAN configurations before enable VLAN trunking. Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DES-3200-28:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DES-3200-28:4# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DES-3200-28:4#
```

show vlan_trunk

Purpose	Used to display VLAN trunk configuration.
Syntax	show vlan_trunk
Description	This command is used to display VLAN trunk information.
Parameters	None.
Restrictions	None.

Example usage:

To display VLAN Trunk information:

```
DES-3200-28:4#show vlan_trunk
Command: show vlan_trunk

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

DES-3200-28:4#
```

Q-IN-Q COMMANDS

The Q-in-Q commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
enable qinq	
disable qinq	
show qinq	
show qinq ports	{<portlist>}
config qinq ports	[<portlist> all] {role [uni nni] outer_tpid <hex 0x1–0xffff> trust_cvid [enable disable] vlan_translation [enable disable]} (1)
create vlan_translation	[add cvid <vidlist> svid <vlanid 1-4094> replace cvid <vlanid 1-4094 svid <vlanid 1-4094>]
delete vlan_translation cvid	[<vidlist> all]
show vlan_translation cvid	{<vidlist>}
config bpdu_tunnel ports	[<portlist> all] type [tunnel {stp gvrp} uplink none]
show bpdu_tunnel	
enable bpdu_tunnel	
disable bpdu_tunnel	

Each command is listed, in detail, in the following sections:

enable qinq

Purpose	This command is used to enable the Q-in-Q mode.
Syntax	enable qinq
Description	<p>This command is used to enable Q-in-Q mode.</p> <p>When Q-in-Q is enabled, all network port roles will be NNI port and their outer TPID will be set to 88a8. All existing static VLANs will run as SP-VLAN. All dynamically learned L2 address will be cleared. GVRP and STP need to be disabled manually.</p> <p>If you need to run GVRP on the Switch, firstly enable GVRP manually. The default setting of Q-in-Q is disabled</p>
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable Q-in-Q:

```
DES-3200-28:4#enable qinq
Command: enable qinq

Success.

DES-3200-28:4#
```

disable qinq

Purpose	This command is used to disable Q-in-Q mode.
Syntax	disable qinq
Description	<p>This command is used to disable Q-in-Q mode.</p> <p>All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared, GVRP will be disabled.</p> <p>If you need to run GVRP on the Switch, firstly enable GVRP manually. All existing SP-VLANs will run as static 1Q VLANs. The default setting of Q-in-Q is disabled.</p>
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable Q-in-Q:

```
DES-3200-28:4#disable qinq
Command: disable qinq

Success.

DES-3200-28:4#
```

show qinq

Purpose	Used to show global Q-in-Q
Syntax	show qinq
Description	This command is used to show the global Q-in-Q status.

show qinq

Parameters	None.
Restrictions	None.

Example usage:

To show global Q-in-Q status:

```
DES-3200-28:4#show qinq
Command: show qinq

Qinq Status: Enabled

DES-3200-28:4#
```

show qinq ports

Purpose	Used to show global Q-in-Q and port Q-in-Q mode status.
Syntax	show qinq ports {<portlist>}
Description	This command is used to show the global Q-in-Q status, including: port role in Q-in-Q mode and port outer TPID.
Parameters	<portlist> - Specifies a range of ports to be displayed. If no parameter is specified, the system will display all Q-in-Q port information.
Restrictions	None.

Example usage:

To show the Q-in-Q status for ports 1 to 4:

```
DES-3200-28:4#show qinq ports 1-4
Commands: show qinq ports 1-4

Port  Role  Outer TPID  Trust_CVID  VLAN  Translation
-----
1      NNI    0x88a8    Disabled    Disabled
2      NNI    0x88a8    Disabled    Disabled
3      NNI    0x88a8    Disabled    Disabled
4      NNI    0x88a8    Disabled    Disabled

Total Entries   : 4

DES-3200-28:4#
```

config qinq ports

Purpose	Used to configure Q-in-Q ports.
Syntax	config qinq ports [<portlist> all] {role [nni uni] outer_tpid <hex 0x1 - 0xffff> trust_cvid [enable disable] vlan_translation [enable disable]} (1)
Description	This command is used to configure the port level setting for the Q-in-Q VLAN function. This setting is not effective when the Q-in-Q mode is

config qinq ports

	disabled.
Parameters	<p><portlist> - A range of ports to configure.</p> <p>role - Port role in Q-in-Q mode, it can be UNI port or NNI port.</p> <p>outer_tpid - TPID in the SP-VLAN tag.</p> <p>trust_cvid - For C-Tag packets, trust C-VID determines if S-VID is enabled. Otherwise, the default is disabled.</p> <p>vlan_translation - If specified as enabled, the VLAN translation will be performed on the port. The setting is disabled by default.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure port list 1 to 4 as NNI port, set outer TPID to 0x88a8:

```
DES-3200-28:4#config qinq ports 1-4 role nni outer_tpid 0x88a8
Command: config qinq ports 1-4 role nni outer_tpid 0x88a8

Warning: The outer TPID will be globally applied to all ports!

Success.

DES-3200-28:4#
```

create vlan_translation

Purpose	Used to create a VLAN translation rule that will be added as a new rule or replace a current rule.
Syntax	create vlan_translation [add cvid <vidlist> svid <vlanid 1-4094> replace cvid <vlanid 1-4094> svid <vlanid 1-4094>]
Description	This command is used to create a VLAN translation rule to add to or replace the outgoing packet which is single S-tagged (the C-VID changes to S-VID and the packet's TPID changes to an outer TPID).
Parameters	<p>cvid – C-VLAN ID of packets that ingress from a UNI port.</p> <p>svid – The S-VLAN ID that replaces the C-VLAN ID or is inserted in the packet.</p> <p><vlanid 1-4094> - A VLAN ID between 1 and 4094.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a VLAN translation rule which assigns add S-VLAN 100 to C-VLAN 1-10:

```
DES-3200-28:4#create vlan_translation add cvid 1-10 svid 100
Command: create vlan_translation add cvid 1-10 svid 100

Success.

DES-3200-28:4#
```

delete vlan_translation cvid

Purpose	Used to delete VLAN translation rules.
Syntax	delete vlan_translation cvid [<vidlist> all]
Description	This command is used to delete VLAN translation rules.
Parameters	cvid - Specifies C-VID rules in VLAN translation.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete all C-VID VLAN translation rules:

```
DES-3200-28:4#delete vlan_translation cvid all

Command: delete vlan_translation cvid all

Success.

DES-3200-28:4#
```

show vlan_translation cvid

Purpose	Used to show VLAN translation rules.
Syntax	show vlan_translation cvid {<vidlist>}
Description	The command used to show configured VLAN translation configurations.
Parameters	cvid - The Q-in-Q translation rules for the specified C-VID list.
Restrictions	None.

Example usage:

To show VLAN translation rules for C-VID 10 to C-VID 40:

```
DES-3200-28:4#show vlan_translation cvid 10-40
Command: show vlan_translation cvid 10-40

CVID   SVID   Action
----   ----   -
10     100    Add
20     100    Add
30     200    Add
40     400    Replace

Total Entries: 4

DES-3200-28:4#
```

config bpdu_tunnel ports	
Purpose	Used to configure the BPDU tunneling port setting.
Syntax	config bpdu_tunnel ports [<portlist> all] type [tunnel {stp gvrp} uplink none]
Description	<p>BPDU tunneling is used to tunnel layer 2 protocol packets. This command is used to configure BPDU tunneling port type. When the device is operated with Q-in-Q enabled, DA will be replaced by the tunnel multicast address, and the BPDU will be tagged with the tunnel VLAN based on the Q-in-Q VLAN configuration and the tunnel/uplink setting.</p> <p>When the device is operated without Q-in-Q enabled, the BPDU will have its DA replaced by the tunnel multicast address and be transmitted out based on the VLAN configuration and the tunnel/uplink setting.</p> <p>The tunnel multicast address for STP BPDU is 01-05-5d-00-00-00. The tunnel multicast address for GVRP BPDU is 01-05-5d-00-00-21.</p>
Parameters	<p>ports - Specify the ports on which the BPDU tunneling will be enabled or disabled.</p> <p>type - Specify the type on the ports.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure BPDU tunneling tunnel ports:

```
DES-3200-28:4#config bpdu_tunnel ports 1-4 type tunnel stp
Command: config bpdu_tunnel ports 1-4 type tunnel stp

Success.

DES-3200-28:4#
```


show bpdu_tunnel

Purpose	Used to show the BPDU Tunneling global state, tunnel destination MAC address, and port state.
Syntax	show bpdu_tunnel
Description	This command is used to show the BPDU Tunneling global state, tunnel destination MAC address, and port state.
Parameters	None.
Restrictions	None.

Example usage:

To show the BPDU tunneling state of all ports:

```
DES-3200-28:4#show bpdu_tunnel
Command: show bpdu_tunnel

BPDU Tunnel : Enabled
STP Tunnel Multicast Address : 01:05:5D:00:00:00
STP Tunnel Port : 1,2
GVRP Tunnel Multicast Address : 01:05:5D:00:00:21
GVRP Tunnel Port :
Uplink Port :

DES-3200-28:4#
```

enable bpdu_tunnel

Purpose	Used to enable BPDU tunneling.
Syntax	enable bpdu_tunnel
Description	This command is used to enable the BPDU tunneling function. By default, it is disabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable BPDU tunneling:

```
DES-3200-28:4#enable bpdu_tunnel
Command: enable bpdu_tunnel

Success.

DES-3200-28:4#
```

disable bpdu_tunnel

Purpose	Used to disable BPDU tunneling.
Syntax	disable bpdu_tunnel
Description	The command is used to disable the BPDU tunneling function.
Parameters	None.

disable bpdu_tunnel

Restrictions Only Administrator-level users can issue this command.

Example usage:

To disable BPDU tunneling:

```
DES-3200-28:4#disable bpdu_tunnel
Command: disable bpdu_tunnel

Success.

DES-3200-28:4#
```

ASYMMETRIC VLAN COMMANDS

The Asymmetric VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	

Each command is listed, in detail, in the following sections:

enable asymmetric_vlan

Purpose	Used to enable asymmetric VLANs on the Switch.
Syntax	enable asymmetric_vlan
Description	This command is used to enable the asymmetric VLAN function on the Switch
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable asymmetric VLANs:

```
DES-3200-28:4#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DES-3200-28:4#
```

disable asymmetric_vlan

Purpose	Used to disable asymmetric VLANs on the Switch.
Syntax	disable asymmetric_vlan
Description	This command is used to disable the asymmetric VLAN function on the Switch
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable asymmetric VLANs:

```
DES-3200-28:4#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DES-3200-28:4#
```

show asymmetric_vlan

Purpose	Used to view the asymmetric VLAN state on the Switch.
Syntax	show asymmetric_vlan
Description	This command is used to display the asymmetric VLAN state on the Switch
Parameters	None.
Restrictions	None.

Example usage:

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

```
DES-3200-28:4#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN: Enabled

DES-3200-28:4#
```

MLD SNOOPING COMMANDS

The MLD Snooping commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config mld_snooping	[vlan <vlan_name 32> vlanid <vidlist> all] { state [enable disable] fast_done [enable disable] } (1)
config mld_snooping querier	[vlan <vlan_name 32> vlanid <vidlist> all] { query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_listener_query_interval <sec 1-25> state [enable disable] version <value 1-2>} (1)
config mld_snooping mrouter_ports	<vlan_name 32> [add delete] <portlist>
config mld_snooping mrouter_ports_forbidden	<vlan_name 32> [add delete] <portlist>
enable mld_snooping	
disable mld_snooping	
show mld_snooping	{vlan <vlan_name 32> vlanid <vidlist>}
show mld_snooping group	{vlan <vlan_name 32> vlanid <vidlist>}
show mld_snooping mrouter_ports	{vlan <vlan_name 32> vlanid <vidlist>} { [static dynamic forbidden]}

Each command is listed, in detail, in the following sections.

config mld_snooping

Purpose	Used to configure MLD snooping on the Switch.
Syntax	config mld_snooping [vlan <vlan_name 32> vlanid <vidlist> all] { state [enable disable] fast_done [enable disable] } (1)
Description	This command is used to configure MLD snooping on the Switch.
Parameters	<p><vlan_name 32> - The name of the VLAN for which MLD snooping is to be configured.</p> <p><vidlist> - The range of VIDs to be configured.</p> <p>all – Select to configure all the VLANs on the Switch.</p> <p>state - Allows you to enable or disable the MLD snooping function for the chosen VLAN.</p> <p>fast_done - Enable or disable the MLD snooping fast done function. If enabled, the membership is immediately removed when the system receives the MLD done message.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the MLD snooping to the default VLAN with the state enabled:

```
DES-3200-28:4#config mld_snooping vlan default state enable
```

```
Command: config mld_snooping vlan default state enable
```

```
Success.
```

```
DES-3200-28:4#
```

config mld_snooping querier

Purpose	Used to configure the timers and the attributes of the MLD snooping querier.
Syntax	config mld_snooping querier [vlan <vlan_name 32> vlanid <vidlist> all] {query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_listener_query_interval <sec 1-25> state [enable disable] version <value 1-2>} (1)
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 guarantees by MLD snooping.
Parameters	<p><vlan_name 32> - The name of the VLAN for which MLD snooping is to be configured.</p> <p><vidlist> - The list of VIDs.</p> <p>all – Select to configure all the VLANs on the Switch.</p> <p>query_interval - Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p>max_reponse_time - The maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.</p> <p>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:</p> <ul style="list-style-type: none"> • Group listener interval—Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval). • Last listener query count—Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. <p>By default, the robustness variable is set to 2. Increase this value if a subnet is expected to be lossy.</p> <p>last_listener_query_interval - The maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group.</p> <p>state - This allows the switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.</p> <p>version <value 1-2> - Specifies the version of MLD packet that will be sent by this port.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the MLD snooping querier query interval to 125 seconds and state enable:

```
DES-3200-28:4#config mld_snooping querier vlan default query_interval 125
state enable
Command: config mld_snooping querier vlan default query_interval 125 state
enable

Success.

DES-3200-28:4#
```

config mld_snooping mrouter_ports

Purpose	Used to configure ports as router ports.
Syntax	config mld_snooping mrouter_ports <vlan_name 32> [add delete] <portlist>
Description	This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	<vlan_name 32> - The name of the VLAN on which the router port resides. [add delete] - Specifies to add or delete the router ports. <portlist> - Specifies a range of ports to be configured.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set up a port range of 1 to 10 to be static router ports:

```
DES-3200-28:4# config mld_snooping mrouter_ports default add 1-10
Command: config mld_snooping mrouter_ports default add 1-10

Success.

DES-3200-28:4#
```

config mld_snooping mrouter_ports_forbidden

Purpose	Used to configure ports as forbidden router ports.
Syntax	config mld_snooping mrouter_ports_forbidden <vlan_name 32> [add delete] <portlist>
Description	This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Parameters	<vlan_name 32> - The name of the VLAN on which the forbidden router port resides. [add delete] - Specifies to add or delete the forbidden router ports. <portlist> - Specifies a range of ports to be configured.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set up port range 1 to 10 to be forbidden router ports:

```
DES-3200-28:4#config mld_snooping mrouter_ports_forbidden default add 1-10
Command: config mld_snooping mrouter_ports_forbidden default add 1-10

Success.

DES-3200-28:4#
```

enable mld_snooping

Purpose	Used to enable MLD snooping on the Switch.
Syntax	enable mld_snooping
Description	This command is used to enable MLD snooping on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable MLD snooping on the Switch:

```
DES-3200-28:4# enable mld_snooping
Command: enable mld_snooping

Success.

DES-3200-28:4#
```

disable mld_snooping

Purpose	Used to disable MLD snooping on the Switch.
Syntax	disable mld_snooping
Description	This command is used to disable MLD snooping on the Switch. Disabling MLD snooping allows all MLD and IPv6 multicast traffic to flood within a Switch by default.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable MLD snooping on the Switch:

```
DES-3200-28:4# disable mld_snooping
Command: disable mld_snooping

Success.

DES-3200-28:4#
```

show mld_snooping

Purpose	Used to display the current configuration of MLD snooping on the Switch.
Syntax	show mld_snooping {vlan <vlan_name 32> vlanid <vidlist>}
Description	This command is used to display the current MLD snooping

show mld_snooping

	configuration on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN for which you want to view the MLD snooping configuration.</p> <p><vidlist> - A list of VIDs.</p> <p>If no parameter specified, the system will display all current MLD snooping configuration.</p>
Restrictions	None.

Example usage:

To display MLD snooping:

```
DES-3200-28:4# show mld_snooping
Command: show mld_snooping

MLD Snooping Global State      : Enabled

VLAN Name                      : default
Query Interval                 : 125
Max Response Time              : 10
Robustness Value               : 2
Last Listener Query Interval  : 1
Querier Router Behavior       : Non-Querier
State                          : Disabled
Fast Done                     : Disabled
Receive Query Count           : 0
Version                        : 2

Total Entries: 1

DES-3200-28:4#
```

show mld_snooping group

Purpose	Used to display the current MLD snooping group configuration on the Switch.
Syntax	show mld_snooping group {[vlan <vlan_name 32> vlanid <vidlist>]}
Description	This command is used to display the current MLD snooping group configuration on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN to view MLD snooping group configuration information.</p> <p><vidlist> - The VIDs to view MLD snooping group configuration information.</p> <p>If no parameters are specified, the system will display all current MLD group snooping configurations of the Switch.</p>
Restrictions	None.

Example usage:

To display MLD snooping groups:

```
DES-3200-28:4#show mld_snooping group
Command: show mld_snooping group

Source/Group      : 2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID     : default/1
Port Member       : 1-2
Mode              : INCLUDE

Source/Group      : 2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID     : default/1
Port Member       : 3
Mode              : EXCLUDE

Source/Group      : NULL/FF0E::100:0:0:21
VLAN Name/VID     : default/1
Port Member       : 4-5
Mode              : EXCLUDE

DES-3200-28:4#
```

show mld_snooping mrouter_ports

Purpose	Used to display the currently configured router ports on the Switch.
Syntax	show mld_snooping mrouter_ports {vlan <vlan_name 32> vlanid <vidlist>} {static dynamic forbidden}
Description	This command is used to display the currently configured router ports on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the router port resides to view information for.</p> <p><vidlist> – The VIDs of the configured routers to view information for.</p> <p>static – Displays router ports that have been statically configured.</p> <p>dynamic – Displays router ports that have been dynamically</p>

show mld_snooping mrouter_ports

configured.

forbidden – Displays forbidden router ports that have been statically configured.

If no parameters are specified, the system will display all currently configured router ports on the Switch.

Restrictions

None.

Example usage:

To display the router ports:

```
DES-3200-28:4# show mld_snooping mrouter_ports
```

```
Command: show mld_snooping mrouter_ports
```

```
VLAN Name           : default
```

```
Static Router Port  : 1-10
```

```
Dynamic Router Port :
```

```
Forbidden Router Port :
```

```
VLAN Name           : vlan2
```

```
Static Router Port  :
```

```
Dynamic Router Port :
```

```
Forbidden Router Port :
```

```
Total Entries : 2
```

```
DES-3200-28:4#
```

IGMP SNOOPING MULTICAST VLAN COMMANDS

The IGMP Snooping Multicast VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
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> tag_member_port <portlist> source_port <portlist> untag_source_port <portlist>] state [enable disable] replace_source_ip [<ipaddr> none] remap_priority [<value 0-7> none] {replace_priority}} (1)
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add <mcast_address_list> delete [<mcast_address_list> all]]
show igmp_snooping multicast_vlan_group	{<vlan_name 32>}
delete igmp_snooping multicast_vlan	<vlan_name 32>
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
show igmp_snooping multicast_vlan	{<vlan_name 32>}

Each command is listed, in detail, in the following sections:

create igmp_snooping multicast_vlan	
Purpose	Used to create a multicast VLAN
Syntax	create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> none] {replace_priority}}
Description	<p>This command is used to create a multicast VLAN. Multiple multicast VLANs can be configured.</p> <p>The ISM VLAN being created cannot exist in the 1Q VLAN database. Multiple ISM VLANs can be created. The ISM VLAN snooping function co-exist with the 1Q VLAN snooping function.</p>
Parameters	<p><vlan_name 32> – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.</p> <p><vlanid 2-4094> – The VLAN ID of the multicast VLAN to be created. The range is 2 to 4094.</p> <p>remap_priority – 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.</p> <p>replace_priority – Specifies that packet's priority will be changed by the switch based on the remap priority. This flag will only take effect when remap priority is set.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an IGMP snooping multicast VLAN with the VLAN name “mv1” and a VLAN ID of 2:

```
DES-3200-28:4# create igmp_snooping multicast_vlan mv1 2
Command: create igmp_snooping multicast_vlan mv1 2

Success.

DES-3200-28:4#
```

config igmp_snooping multicast_vlan	
Purpose	Used to configure the parameter of the specific multicast VLAN.
Syntax	config igmp_snooping multicast_vlan <vlan_name 32> { [add delete] [member_port <portlist> tag_member_port <portlist> source_port <portlist> untag_source_port <portlist>] state [enable disable] replace_source_ip [<ipaddr> none] remap_priority [<value 0-7> none] {replace_priority}} (1)
Description	<p>This command is used to add a member port, add a tagged member port, add a source port, and add an untagged source port to the port list. The member port and the untagged source port will automatically become untagged members of the multicast VLAN; the tagged member port and the source port will automatically become the tagged members of the multicast VLAN. To change the port list, add or delete it.</p> <p>The member port list and source port list can not overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN.</p> <p>The multicast VLAN must be created first before configuration.</p>
Parameters	<p><vlan_name 32> – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.</p> <p>[add delete] - Add or delete the ports to the multicast VLAN.</p> <p>member_port – A range of member ports to add to the multicast VLAN. They will become the untagged member port of the ISM VLAN.</p> <p>tag_member_port - Specifies the tagged member port of the ISM VLAN.</p> <p>source_port - A range of source ports to add to the multicast VLAN.</p> <p>untag_source_port - A range of untagged source ports to add to the multicast VLAN. The reassigned PVID of the untagged source port will be automatically changed to the multicast VLAN.</p> <p>state - Enable or disable multicast VLAN for the chosen VLAN.</p> <p>replace_source_ip - With the IGMP snooping function, the IGMP report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address. If none is specified, the source IP address will not be replaced.</p> <p>remap_priority - The remap priority value (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.</p> <p>replace_priority - Specifies that packet’s priority will be changed by the Switch based on the remap priority. This flag will only take effect when remap priority is set.</p>
Restrictions	Only Administrator-level users can issue this command.


Example usage:

To configure an IGMP snoop multicast VLAN:

```
DES-3200-28:4# config igmp_snooping multicast_vlan v1 add member_port 1,3
state enable
Command: config igmp_snooping multicast_vlan v1 add member_port 1,3 state
enable

Success.

DES-3200-28:4#
```

config igmp_snooping multicast_vlan multicast_group	
Purpose	Used to configure the multicast group which will be learned with the specific multicast VLAN.
Syntax	config igmp_snooping multicast_vlan_group <vlan_name 32> [add <mcast_address_list> delete [<mcast_address_list> all]]
Description	This command is used to configure the multicast group which will be learned with the specific multicast VLAN. There are two cases need to be considered. The join packet will be learned with the multicast VLAN that contain the destination multicast group. If the destination multicast group of the join packet can not be classified into any multicast VLAN that this port belong, then the join packet will be learned with the natural VLAN of the packet.
Parameters	<div style="display: flex; align-items: flex-start;"> <div style="text-align: center; margin-right: 10px;">  </div> <div> <p>Note: <i>The same multicast group can not be overlapped in different multicast VLANs. Multiple multicast groups can be added to a multicast VLAN.</i></p> </div> </div> <p><vlan_name 32> – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters.</p> <p><mcast_address_list> - Add or delete the list of multicast groups that will be learned with the specified multicast VLAN.</p> <p>all - All multicast groups will be deleted from the specified multicast VLAN.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a group to a multicast VLAN:

```
DES-3200-28:4#config igmp_snooping multicast_vlan_group v1 add 225.1.1.1
Command: config igmp_snooping multicast_vlan_group v1 add 225.1.1.1

Success.

DES-3200-28:4#
```

show igmp_snooping multicast_vlan_group

Purpose	Used to display the multicast groups configured for the specified multicast VLAN.
Syntax	show igmp_snooping multicast_vlan_group {<vlan_name 32>}
Description	This command is used to display the multicast groups configured for the specified multicast VLAN.
Parameters	<vlan_name 32> - The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters. If no parameters are specified, the system will display all multicast VLAN groups on the Switch.
Restrictions	None.

Example usage:

To display the multicast groups configured for a multicast VLAN:

```
DES-3200-28:4#show igmp_snooping multicast_vlan_group v1
Command: show igmp_snooping multicast_vlan_group v1

VLAN Name      VLAN ID      From          To
-----
v1             100          224.19.62.34 224.19.162.200

DES-3200-28:4#
```

delete igmp_snooping multicast_vlan

Purpose	Used to delete a multicast VLAN.
Syntax	delete igmp_snooping multicat_vlan <vlan_name 32>
Description	This command is used to delete a multicast VLAN.
Parameters	<vlan_name 32> - The name of the multicast VLAN to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an IGMP snoop multicast VLAN:

```
DES-3200-28:4# delete igmp_snooping multicat_vlan v1
Command: delete igmp_snooping multicat_vlan v1

Success.

DES-3200-28:4#
```

enable igmp_snooping multicast_vlan

Purpose	Used to enable the multicast VLAN function.
Syntax	enable igmp_snooping multicast_vlan
Description	This command is used to control the multicast VLAN function. The ISM VLAN will take effect when IGMP snooping multicast VLAN is enabled. By default, the multicast VLAN is in a disabled state.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable an IGMP snoop multicast VLAN:

```
DES-3200-28:4# enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DES-3200-28:4#
```

disable igmp_snooping multicast_vlan

Purpose	Used to disable the multicast VLAN function.
Syntax	disable igmp_snooping multicast_vlan
Description	This command is used to disable the multicast VLAN function. By default, the multicast VLAN is in a disabled state.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable IGMP snoop multicast VLAN:

```
DES-3200-28:4# disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DES-3200-28:4#
```

show igmp_snooping multicast_vlan

Purpose	Used to view multicast VLAN information.
Syntax	show igmp_snooping multicast_vlan {<vlan_name 32>}
Description	This command is used to display multicast VLAN information.
Parameters	<vlan_name 32> – The name of the multicast VLAN to be shown. If no parameters are specified, the system will display all multicast VLANs on the Switch.
Restrictions	None.

Example usage:

To display IGMP snooping multicast VLAN information:


```
DES-3200-28:4# show igmp_snooping multicast_vlan
```

```
Command: show igmp_snooping multicast_vlan
```

```
Multicast VLAN Global State : Enabled
```

```
VID : 4001 VLAN Name: 4001
```

```
Member Ports : 7-10
```

```
Tagged Member Ports : 11-18
```

```
Source Ports : 21-26
```

```
Untagged Source Ports : 1-6,27
```

```
Status : Enabled
```

```
Replace Source IP : 10.90.90.100
```

```
Priority : 7 (Replace)
```

```
VID : 4002 VLAN Name: 4002
```

```
Member Ports :
```

```
Tagged Member Ports :
```

```
Source Ports :
```

```
Untagged Source Ports :
```

```
Status : Disabled
```

```
Replace Source IP : None
```

```
Priority : None
```

```
DES-3200-28:4#
```

LIMITED IP MULTICAST ADDRESS COMMANDS

The Limited IP Multicast Address commands allows the administrator to permit or deny access to a port or range of ports by specifying a range of multicast addresses. The limited IP multicast address commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
create mcast_filter_profile	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)
delete mcast_filter_profile	profile_id [<value 1-24> all]
delete mcast_filter_profile	profile_name <name 1-32>
show mcast_filter_profile	{profile_id <value 1-24> profile_name <name 1-32> }
config limited_multicast_addr ports	<portlist> {[add delete] [profile_id <value 1-24> profile_name <name 1-32>] access [permit deny]} (1)
show limited_multicast_addr	ports {<portlist>}
config max_mcast_group	ports <portlist> max_group <value 1-1024>
show max_mcast_group	ports {<portlist>}

Each command is listed, in detail, in the following sections:

create mcast_filter_profile	
Purpose	Used to create a multicast address profile.
Syntax	create mcast_filter_profile profile_id <value 1-24> profile_name <name 1-32>
Description	This command is used to create a multicast address profile with a profile ID and profile name.
Parameters	profile_id – ID of the profile. The range is 1 to 24. profile_name – Provides a description for the profile.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a multicast range profile with a profile ID and a profile name:

```
DES-3200-28:4#create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

DES-3200-28:4#
```

config mcast_filter_profile	
Purpose	Used to add or delete a range of multicast addresses to the profile.
Syntax	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)
Description	This command is used to add or delete a range of multicast addresses to the profile.
Parameters	<p>profile_id – The ID of the profile.</p> <p>profile_name – Provides a description for the profile.</p> <p>[add delete] – Add or delete the list of the multicast addresses to the profile.</p> <p><mcast_address_list> – List of the multicast addresses to be put in the profile. Specify a single multicast IP address or a range of multicast addresses.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add the multicast address range 225.1.1.1-225.1.1.10 to profile ID 2:

```
DES-3200-28:4#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-3200-28:4#
```

delete mcast_filter_profile	
Purpose	Used to delete a multicast address profile.
Syntax	delete mcast_filter_profile profile_id [<value 1-24> all]
Description	This command is used to delete a multicast address profile.
Parameters	<p>profile_id – The ID of the profile.</p> <p>all – All multicast address profiles will be deleted.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a multicast range profile with profile ID 3:

```
DES-3200-28:4# delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3

Success.

DES-3200-28:4#
```

delete mcast_filter_profile

Purpose	Used to delete a multicast address profile.
Syntax	delete mcast_filter_profile profile_name <name 1-32>
Description	This command is used to delete a multicast address profile.
Parameters	profile_name – Name of the profile.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a multicast range profile with the profile name “shipping”:

```
DES-3200-28:4# delete mcast_filter_profile profile_name shipping
Command: delete mcast_filter_profile profile_name shipping

Success.

DES-3200-28:4#
```

show mcast_filter_profile

Purpose	Used to display the defined multicast address profiles.
Syntax	show mcast_filter_profile {profile_id <value 1-24> profile_name <name 1-32> }
Description	This command is used to display the defined multicast address profiles.
Parameters	profile_name – Specifies to display a profile based on a profile name. profile_id – ID of the profile. If not specified, all profiles will be displayed.
Restrictions	None.

Example usage:

To display the multicast filter profile:

```
DES-3200-28:4#show mcast_filter_profile
```

```
Command: show mcast_filter_profile
```

```
Mcast Filter Profile:
```

```
Profile ID Name                               Multicast Addresses
-----
1          m1                                234.1.1.1-234.1.1.10 ,
                                           234.2.1.1-234.2.1.100
```

```
Profile ID Name                               Multicast Addresses
-----
2          m2                                239.1.10.1-239.1.10.5
```

```
Total Profile Count: 2
```

```
DES-3200-28:4#
```

config limited_multicast_addr ports

Purpose	Used to configure the multicast address filtering function on a port.
Syntax	config limited_multicast_addr ports <portlist> { [add delete] [profile_id <value 1-24> profile_name <name 1-32>] access [permit deny] } (1)
Description	This command is used to configure the multicast address filtering function on a port. When there are no profiles specified with a port, the limited function is not effective.
Parameters	<portlist> - A port or range of ports on which the limited multicast address range to be configured has been assigned. add – Add a multicast address profile to a port. delete – Delete a multicast address profile to a port. profile_id – A profile ID to be added or deleted from a port. profile_name – A profile name to be added or deleted from a port. permit – Specifies that the packet that matches the addresses defined in the profiles will be permitted. The default mode is permit. deny - Specifies that the packet that matches the addresses defined in the profiles will be denied.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure ports 1 and 3 to set the multicast address profile 2:

```
DES-3200-28:4#config limited_multicast_addr ports 1,3 add profile_id 2
```

```
Command: config limited_multicast_addr ports 1,3 add profile_id 2
```

```
Success.
```

```
DES-3200-28:4#
```

show limited_multicast_addr

Purpose	Used to show the per-port Limited IP multicast address range.
----------------	---

show limited_multicast_addr	
Syntax	show limited_multicast_addr ports {<portlist>}
Description	This command is used to display the multicast filter profiles bound to ports.
Parameters	<portlist> - A port or range of ports on which the limited multicast address range to be shown has been assigned. If no portlists are specified, the system will display all ports on which the limited multicast address range is to be shown.
Restrictions	None.

Example usage:

To show the limited multicast address on ports 1 and 3:

```
DES-3200-28:4#show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Port : 1
Access: permit

Profile ID Name                               Multicast Addresses
-----
Port : 3
Access: permit

Profile ID Name                               Multicast Addresses
-----

DES-3200-28:4#
```

config max_mcast_group	
Purpose	Used to configure the maximum number of multicast groups a port can join.
Syntax	config max_mcast_group ports <portlist> max_group <value 1-1024>
Description	This command is used to configure the maximum number of multicast groups that a port can join.
Parameters	<portlist> - A range of ports to configure the maximum multicast group. max_group - Specifies the maximum number of multicast groups. The range is from 1 to 1024. 1024 is the default setting.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the maximum multicast address groups on ports 1 and 3 as 100:

```
DES-3200-28:4#config max_mcast_group ports 1,3 max_group 100
Command: config max_mcast_group ports 1,3 max_group 100

Success.

DES-3200-28:4#
```

show max_mcast_group

Purpose	Used to display the maximum number of multicast groups that a port can join.
Syntax	show max_mcast_group ports {<portlist>}
Description	This command is used to display the maximum number of multicast groups that a port can join.
Parameters	<portlist> - A range of ports to display the maximum number of multicast groups. If no portlists are specified, the system will display the maximum number of multicast groups for all ports.
Restrictions	None.

Example usage:

To display the maximum number of multicast groups on port 1:

```
DES-3200-28:4#show max_mcast_group ports 1
Command: show max_mcast_group ports 1

Max Multicast Filter Group:
Port      MaxMcastGroup
----      -
1         1024

DES-3200-28:4#
```

LLDP COMMANDS

The LLDP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
enable lldp	
disable lldp	
config lldp message_tx_interval	<sec 5 - 32768 >
config lldp message_tx_hold_multiplier	< int 2 - 10 >
config lldp tx_delay	< sec 1 - 8192 >
config lldp reinit_delay	< sec 1 - 10 >
config lldp notification_interval	<sec 5 - 3600 >
config lldp ports	[<portlist> all] notification [enable disable]
config lldp ports	[<portlist> all] admin_status [tx_only rx_only tx_and_rx disable]
config lldp ports	[<portlist> all] mgt_addr ipv4 <ipaddr> [enable disable]
config lldp ports	[<portlist> all] basic_tlvs [all {port_description system_name system_description system_capabilities}] [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_pvid [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_protocol_vid [vlan [all <vlan_name 32>] vlanid <vlanid_list>] [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_vlan_name [vlan [all <vlan_name 32>] vlanid <vlanid_list>] [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_protocol_identity [all { eapol lacp gvrp stp }] [enable disable]
config lldp ports	[<portlist> all] 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>}
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>}

Each command is listed, in detail, in the following sections:

enable lldp

Purpose	Used to enable LLDP operations on the Switch.
Syntax	enable lldp
Description	<p>This command is used for global control of the LLDP function.</p> <p>When this function is enabled, the Switch can start to transmit LLDP packets and receive and process the LLDP packets.</p> <p>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.</p> <p>The default state for LLDP is disabled.</p>
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable LLDP:

```
DES-3200-28:4# enable lldp
Command: enable lldp

Success.

DES-3200-28:4#
```

disable lldp

Purpose	Used to disable LLDP operation on the Switch.
Syntax	disable lldp
Description	<p>This command is used to stop the sending and receiving of LLDP advertisement packets.</p>
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable LLDP:

```
DES-3200-28:4# disable lldp
Command: disable lldp

Success.

DES-3200-28:4#
```

config lldp message_tx_interval

Purpose	Used to change the packet transmission interval.
Syntax	config lldp message_tx_interval <sec 5-32768>
Description	This command is used to control how often active ports retransmit advertisements to their neighbors.
Parameters	message_tx_interval - Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The range is from 5 to 32768 seconds. The default setting is 30 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the packet transmission interval:

```
DES-3200-28:4# config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DES-3200-28:4#
```

config lldp message_tx_hold_multiplier

Purpose	This command is used to configure the message hold multiplier.
Syntax	config lldp message_tx_hold_multiplier <int 2-10>
Description	This command is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU. The TTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message_tx_interval * message_tx_hold_multiplier). At the partner switch, when the Time-to-Live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.
Parameters	message_tx_hold_multiplier - The range is from 2 to 10. The default setting 4.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the multiplier value:

```
DES-3200-28:4# config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

DES-3200-28:4#
```

config lldp tx_delay

Purpose	Used to change the minimum time (delay-interval) of any LLDP port. It will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The Tx delay defines the minimum interval between the sending of LLDP messages due to constant changes of MIB content.
Syntax	config lldp tx_delay <sec 1–8192>
Description	The LLDP message_tx_interval (transmit interval) must be greater than or equal to (4 x tx_delay interval).
Parameters	tx_delay - The range is from 1 second to 8192 seconds. The default setting 2 seconds. NOTE: The Tx Delay should be less than or equal to 0.25 * msgTxInterval
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the delay-interval interval:

```
DES-3200-28:4# config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DES-3200-28:4#
```

config lldp reinit_delay

Purpose	Change the minimum time of re-initialization delay interval.
Syntax	config lldp reinit_delay <sec 1–10>
Description	An re-enabled LLDP port will wait for reinit_delay after last disable command before reinitializing
Parameters	reinit_delay - The range is from 1 second to 10 seconds. The default setting 2 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the re-initialization delay interval:

```
DES-3200-28:4# config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DES-3200-28:4#
```

config lldp notification_interval

Purpose	Used to configure the timer of the notification interval used to send notifications to configured SNMP trap receiver(s).
Syntax	config lldp notification_interval <sec 5 - 3600>
Description	Globally change the interval between successive LLDP change notifications generated by the switch.
Parameters	notification_interval - The range is from 5 second to 3600 seconds. The default setting is 5 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the notification interval:

```
DES-3200-28:4# config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DES-3200-28:4#
```

config lldp ports notification

Purpose	Used to configure each port for sending notifications to configured SNMP trap receiver(s).
Syntax	config lldp ports [<portlist> all] notification [enable disable]
Description	Enable or disable each port for sending change notifications to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout and information update. The changed type includes any data update /insert/remove.
Parameters	<portlist> - Specify a range of ports to be configured. all - To set all ports in the system, use the "all" parameter. 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.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the port SNMP notification state:

```
DES-3200-28:4# config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DES-3200-28:4#
```

config lldp ports admin_status

Purpose	Used to configure per-port transmit and receive modes.
Syntax	config lldp ports [<portlist> all] admin_status [tx_only rx_only tx_and_rx disable]
Description	These options enable the Switch to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.
Parameters	<p><portlist> - Specify a range of ports to be configured.</p> <p>all - To set all ports in the system, use the “all” parameter.</p> <p>admin_status:</p> <p>tx_only - Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices.</p> <p>rx_only - Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors.</p> <p>tx_and_rx - Configure the specified port(s) to both transmit and receive LLDP packets.</p> <p>disable - Disable LLDP packet transmit and receive on the specified port(s).</p> <p>The default per port state is tx_and_rx.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the port’s transmit and receive mode:

```
DES-3200-28:4# config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DES-3200-28:4#
```

config lldp ports mgt_addr

Purpose	Used to enable or disable the port(s) which have been specified for advertising the indicated management address instances.
Syntax	config lldp ports [<portlist> all] mgt_addr ipv4 <ipaddr> [enable disable]
Description	This command is used to specify whether the system’s IP address needs to be advertised from the specified port. For layer 3 devices, each managed address can be individually specified. The management addresses that are added in the list will be advertised in the LLDP from the specified interface associated with each management address. The interface for that management address will be also advertised in the if-index form.
Parameters	<p><portlist> - Specify a range of ports to be configured.</p> <p>all - To set all ports in the system, use the “all” parameter.</p> <p>ipv4 - IP address of IPV4.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable port 1 to port 2 to manage address entries:

```
DES-3200-28:4# config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable

Success

DES-3200-28:4#
```

config lldp ports basic_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of the optional TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] basic_tlvs [all {port_description system_name system_description system_capabilities}] [enable disable]
Description	An active LLDP port on the Switch always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end f LLDPDU TLV, chassis ID TLV, port ID TLV, Time to Live TLV). The mandatory type can not be disabled. There are also four data types which can be optionally selected. They are port_description, system_name, system_description, and system_capability.
Parameters	<p><portlist> - Specify a range of ports to be configured.</p> <p>all - To set all ports in the system, use the "all" parameter.</p> <p>port_description - This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled.</p> <p>system_name - This TLV optional data type indicates that the LLDP agent should transmit 'System Name TLV'. The default state is disabled.</p> <p>system_description - This TLV optional data type indicates that the LLDP agent should transmit 'System Description TLV'. The default state is disabled.</p> <p>system_capabilities - This TLV optional data type indicates that the LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router functions, and whether the provided functions are currently enabled. The default state is disabled.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the Switch to exclude the system name TLV from outbound LLDP advertisements on all ports:

```
DES-3200-28:4# config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DES-3200-28:4#
```

config lldp ports dot1_tlv_pvid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port vlan ID TLV data types come
----------------	---

config lldp ports dot1_tlv_pvid

	from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_pvid [enable disable]
Description	This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port.
Parameters	<p><portlist> - Specify a range of ports to be configured.</p> <p>all - To set all ports in the system, use the “all” parameter.</p> <p>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.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28:4# config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DES-3200-28:4#
```

config lldp ports dot1_tlv_protocol_vid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 organization protocol identity TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_protocol_vid [vlan [all all <vlan_name 32>] vlanid <vlanid_list>] [enable disable]
Description	This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations which are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.
Parameters	<p><portlist> - Specify a range of ports to be configured.</p> <p>all - To set all ports in the system, use the “all” parameter.</p> <p>dot1_tlv_protocol_vid - This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.</p> <p>vlanid_list – A list of VIDs to be configured for this command.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28:4# config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DES-3200-28:4#
```

config lldp ports dot1_tlv_vlan_name

Purpose	Used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 Organizational VLAN name TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_vlan_name [vlan [all <vlan_name 32>] vlanid <vidlist>] [enable disable]
Description	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 IDs will be advertised.
Parameters	<portlist> – Specify a range of ports to be configured. all - To set all ports in the system, use the “all” parameter. 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 IDs will be advertised. The default state is disable.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28:4# 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-3200-28:4#
```

config lldp ports dot1_tlv_protocol_identity

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 organization protocol identity TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_protocol_identity [all {eapol lacp gvrp stp }] [enable disable]
Description	This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations which are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.
Parameters	<portlist> - Specify a range of ports to be configured. all - To set all ports in the system, use the “all” parameter. dot1_tlv_protocol_identity - This TLV optional data type indicates whether

config lldp ports dot1_tlv_protocol_identity

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 disable.

Restrictions Only Administrator-level users can issue this command.

Example usage

To configure the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28:4# config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DES-3200-28:4#
```

config lldp ports dot3_tlvs

Purpose Used to configure an individual port or group of ports to exclude one or more of IEEE 802.3 organization specific TLV data types from outbound LLDP advertisements.

Syntax config lldp ports [<portlist>|all] dot3_tlvs [all | {mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]

Description Each Specific TLV in this extension can be enabled individually.

Parameters

- <portlist> - Specify a range of ports to be configured.
- all - To set all ports in the system, use the "all" parameter.
- mac_phy_configuration_status - 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 support 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 - 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 - 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 - This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV'. The default state is disabled.

config lldp ports dot3_tlvs

Restrictions Only Administrator-level users can issue this command.

Example usage

To configure the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DES-3200-28:4#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-3200-28:4#
```

config lldp forward_message

Purpose Used to configure forwarding of LLDP DU packets when LLDP is disabled.

Syntax config lldp forward_message [enable | disable]

Description When LLDP is disabled and LLDP forward message is enabled, the received LLDP DU packets will be forwarded. The default state is disable.

Parameters None.

Restrictions Only Administrator-level users can issue this command.

Example usage

To configure the LLDP forward LLDPDU DU:

```
DES-3200-28:4# config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DES-3200-28:4#
```

show lldp

Purpose This command displays the Switch's general LLDP configuration status.

Syntax show lldp

Description This command is used to display the Switch's general LLDP configuration status.

Parameters None.

Restrictions None.

Example usage

To display the LLDP system level configuration status:

```
DES-3200-28:4# show lldp
Command: show lldp

LLDP system information
  Chassis Id Subtype      : MAC Address
  Chassis Id              : 00-15-E9-41-5A-A7
  System Name             : D-Link
  System Description      : Fast Ethernet Switch
  System Capabilities     : Repeater, Bridge,

LLDP Configurations
  LLDP Status             : Disable
  LLDP Forward Status    : Disable
  Message Tx Interval    : 30
  Message Tx Hold Multiplier : 4
  ReInit delay           : 2
  Tx Delay               : 2
  Notification Interval  : 5

DES-3200-28:4#
```

show lldp mgt_addr	
Purpose	Used to display the LLDP management address information.
Syntax	show lldp mgt_addr {ipv4 <ipaddr>}
Description	This command is used to display LLDP management address information.
Parameters	ipv4 - IP address of IPV4.
Restrictions	None.

Example usage

To display the management address information:

```
DES-3200-28:4# show lldp mgt_addr ipv4 192.168.254.10
Command: show lldp mgt_addr ipv4 192.168.254.10

Total Address:1

DES-3200-28:4#
```

show lldp ports	
Purpose	Used to display the LLDP per port configuration for advertisement options.
Syntax	show lldp ports {<portlist> }
Description	This command is used to display the LLDP per port configuration for advertisement options.
Parameters	<portlist> - Specify a range of ports to be displayed. When port list is not specified, information for all ports will be displayed.
Restrictions	None.

Example usage

To display the LLDP per port TLV option configuration:

```

DES-3200-28:4# show lldp ports 1
Command: show lldp ports 1

Port ID                : 1
-----
Admin Status           : TX_and_RX
Notification Status    : Disable
Advertised TLVs Option :
    Port Description           Disable
    System Name                Disable
    System Description         Disable
    System Capabilities        Disable
    Enabled Management Address
    (NONE.)
    Port VLAN ID              Disable
Enabled Port_and_protocol_VLAN_ID
(NONE)
    Enabled VLAN Name
    (NONE.)
    Enabled protocol_identity
    (NONE.)
    MAC/PHY Configuration/Status      Disable
Power Via MDI                Disable
    Link Aggregation              Disable
    Maximum Frame Size            Disable

DES-3200-28:4#
    
```

show lldp local_ports	
Purpose	Used to display the per-port information currently available for populating outbound LLDP advertisements.
Syntax	show lldp local_ports {<portlist>} {mode [brief normal detailed]}
Description	This command is used to display the per-port information currently available for populating outbound LLDP advertisements.
Parameters	<portlist> - Specify a range of ports to be configured. When a port list is not specified, information for all ports will be displayed. 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 usage

To display outbound LLDP advertisements for individual ports in detail:

```

DES-3200-28:4# show lldp local_ports 1 mode detailed
Command: show lldp local_ports 1 mode detailed

Port ID : 1
-----
Port ID Subtype           : Local
Port ID                   : 1/1
Port Description          : RMON Port 1 on Unit 1
Port PVID                 : 1
Management Address count : 1
    Subtype                : IPv4
    Address                 : 10.73.21.51
    IF Type                 : unknown
    OID                     : 1.3.6.1.4.1.171.10.64.1

PPVID Entries Count      : 0
    (NONE)

VLAN Name Entries count  : 1
    Entry 1 :
        VLAN ID           : 1
        VLAN Name          : default

Protocol Identity Entries count : 1
    Entry 1 :
        Protocol index     : 4
        Protocol ID        : 00 27 42 42 03 00 00 02

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

To display outbound LLDP advertisements for specific ports in normal mode:

```

DES-3200-28:4# show lldp local_ports 1 mode normal
Command: show lldp local_ports 1 mode normal

Port ID : 1:
-----
Port ID Subtype           : Local
Port ID                   : 1/1
Port Description          : RMON Port 1 on Unit 1
Port PVID                 : 1
Management Address count : 1
PPVID Entries Count      : 0
VLAN Name Entries count  : 1
Protocol Identity Entries count : 1
MAC/PHY Configuration/Status : (See detail)
Power Via MDI             : (See detail)
Link Aggregation          : (See detail)
Maximum Frame Size        : 1536

DES-3200-28:4#
    
```

To display outbound LLDP advertisements for specific ports in brief mode:

```

DES-3200-28:4# show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief

Port ID : 1
-----
Port ID Subtype           : Local
Port ID                   : 1/1
Port Description          : RMON Port 1 on Unit 1
DES-3200-28:4#
    
```

show lldp remote_ports

Purpose	Used to display the information learned from the neighbor.
Syntax	show lldp remote_ports {<portlist>} [brief normal detailed]
Description	This command is used to display the information learned from the neighbor parameters. A maximum of 32 VLAN Name entries and 10 Management Address entries can be received.
Parameters	<portlist> - Specify a range of ports to be configured. When a port list is not specified, information for all ports will be displayed. 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 usage

To display remote table entries in brief mode:

```

DES-3200-28:4# show lldp remote_ports 1-2 brief
Command: show lldp remote_ports 1-2 brief

Port ID: 1
-----
Remote Entities Count : 3
Entity 1
    Chassis ID Subtype      : MAC Address
    Chassis ID              : 00-01-02-03-04-01
    Port ID Subtype         : Local
    Port ID                 : 1/3
    Port Description        : RMON Port 1 on Unit 3

Entity 2
    Chassis ID Subtype      : MAC Address
    Chassis ID              : 00-01-02-03-04-02
    Port ID Subtype         : Local
    Port ID                 : 1/4
    Port Description        : RMON Port 1 on Unit 4

Port ID : 2
-----
Remote Entities Count : 3
Entity 1
    Chassis ID Subtype      : MAC Address
    Chassis ID              : 00-01-02-03-04-03
    Port ID Subtype         : Local
    Port ID                 : 2/1
    Port Description        : RMON Port 2 on Unit 1

Entity 2
    Chassis ID Subtype      : MAC Address
    Chassis ID              : 00-01-02-03-04-04
    Port ID Subtype         : Local
    Port ID                 : 2/2
    Port Description        : RMON Port 2 on Unit 2

Entity 3
    Chassis ID Subtype      : MAC Address
    Chassis ID              : 00-01-02-03-04-05
    Port ID Subtype         : Local
    Port ID                 : 2/3
    Port Description        : RMON Port 2 on Unit 3

DES-3200-28:4#
    
```

To display remote table entries in normal mode:

```

DES-3200-28:4# show lldp remote_ports ports 1 normal
Command: show lldp remote_ports ports 1 normal

Port ID : 1
-----
Remote Entities Count : 2
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-01
  Port ID Subtype        : Local
  Port ID                 : 1/3
  Port Description        : RMON Port 3 on Unit 1
  System Name             : Switch1
  System Description      : Stackable Ethernet Switch
  System Capabilities     : Repeater, Bridge
  Management Address Count : 1
  Port VLAN ID           : 1
  PPVID Entries Count     : 5
  VLAN Name Entries Count : 3
  Protocol ID Entries Count : 2
  MAC/PHY Configuration Status : (See Detail)
  Power Via MDI           : (See Detail)
  Link Aggregation        : (See Detail)
  Maximum Frame Size      : 1536
  Unknown TLVs Count     : 2

Entity 2
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-02
  Port ID Subtype        : Local
  Port ID                 : 2/1
  Port Description        : RMON Port 1 on Unit 2
  System Name             : Switch2
  System Description      : Stackable Ethernet Switch
  System Capabilities     : Repeater, Bridge
  Management Address Count : 2
  Port VLAN ID           : 1
  PPVID Entries Count     : 5
  VLAN Name Entries Count : 3
  Protocol ID Entries Count : 2
  MAC/PHY Configuration Status : (See Detail)
  Power Via MDI           : (See Detail)
  Link Aggregation        : (See Detail)
  Maximum Frame Size      : 1536

DES-3200-28:4#
    
```


To display remote table entries in detailed mode:

```

DES-3200-28:4# show lldp remote_ports 1 mode detailed
Command: show lldp remote_ports 1 mode detailed

Port ID : 1
-----
Remote Entities count : 1
Entity 1
  Chassis Id Subtype      : MAC Address
  Chassis Id              : 00-00-00-48-46-29
  Port Id Subtype         : Local
  Port ID                 : 1/16
  Port Description        : RMON Port 16 on Unit 1
  System Name             :
  System Description      : Fast Ethernet Switch
  System Capabilities     : Repeater, Bridge,
  Management Address count : 1
    Entry 1 :
      Subtype      : IPv4
      Address      : 10.48.46.128
      IF Type      : unknown
      OID          : 1.3.6.1.4.1.171.11.63.9

  Port PVID              : 1
  PPVID Entries count   : 0
    (None.)

  VLAN Name Entries count : 1
    Entry 1 :
      Vlan ID        : 1
      Vlan Name      : default

  Protocol ID Entries count : 0
    (None.)

  MAC/PHY Configuration/Status :
    Auto-negotiation support   : supported
    Auto-negotiation status    : enabled
    Auto-negotiation advertised capability : 8000(hex)
    Auto-negotiation operational MAU type : 0010(hex)

  Power Via MDI          :
    Port class           : PSE
    PSE MDI power support : supported
    PSE MDI power state  : enabled
    PSE pairs control ability : uncontrollable
    PSE power pair       : 0
    power class          : 0

  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-3200-28:4#

show lldp statistics

Purpose	Used to display the system LLDP statistics information.
Syntax	show lldp statistics
Description	This command is used to display an overview of neighbor detection activity on the Switch.
Parameters	None.
Restrictions	None.

Example usage

To display global statistics information:

```
DES-3200-28:4# show lldp statistics
Command: show lldp statistics

Last Change Time           : 6094
Number of Table Insert     : 1
Number of Table Delete     : 0
Number of Table Drop       : 0
Number of Table Ageout     : 0

DES-3200-28:4#
```

show lldp statistics ports

Purpose	Used to display the ports LLDP statistics information.
Syntax	show lldp statistics ports {<portlist>}
Description	This command is used to display per-port LLDP statistics.
Parameters	<portlist> - Specify a range of ports to be configured. When a port list is not specified, information for all ports will be displayed.
Restrictions	None.

Example usage

To display statistics information of port 1:

```
DES-3200-28:4# show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID: 1
-----
      lldpStatsTxPortFramesTotal      : 27
      lldpStatsRxPortFramesDiscardedTotal : 0
      lldpStatsRxPortFramesErrors      : 0
      lldpStatsRxPortFramesTotal      : 27
      lldpStatsRxPortTLVsDiscardedTotal : 0
      lldpStatsRxPortTLVsUnrecognizedTotal : 0
      lldpStatsRxPortAgeoutsTotal      : 0

DES-3200-28:4#
```

To display statistics information of port 1:

```
DES-3200-28:4# show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID: 1
-----
      lldpStatsTxPortFramesTotal      : 27
      lldpStatsRxPortFramesDiscardedTotal : 0
      lldpStatsRxPortFramesErrors      : 0
      lldpStatsRxPortFramesTotal      : 27
      lldpStatsRxPortTLVsDiscardedTotal : 0
      lldpStatsRxPortTLVsUnrecognizedTotal : 0
      lldpStatsRxPortAgeoutsTotal      : 0

DES-3200-28:4#
```

DoS PREVENTION COMMANDS

The DoS Prevention commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config dos_prevention dos_type	[{land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024} (1) all] {action [drop mirror <port> {priority <value 0-7> rx_rate [no_limit <value 64-1024000> }] } enable disable]} (1)
show dos_prevention	{land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024}
clear dos_prevention counters	{land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024}
enable dos_prevention trap_log	
disable dos_prevention trap_log	

Each command is listed, in detail, in the following sections:

config dos_prevention dos_type	
Purpose	This command is used to discard the L3 control packets sent to CPU from specific ports.
Syntax	config dos_prevention dos_type [{land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024} (1) all] {action [drop mirror <port> {priority <value 0-7> rx_rate [no_limit <value 64-1024000> }] } enable disable] } (1)
Description	This command is used to configure the prevention of DoS attacks, and includes state and action. The packets matching will be used by the hardware. For a specific type of attack, the content of the packet, regardless of the receipt port or destination port, will be matched against a specific pattern.
Parameters	<p>The type of DoS attack. Possible values are as follows:</p> <ul style="list-style-type: none"> land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024 <p>state - Enable or disable DoS prevention.</p> <p>By default, prevention for all types of DoS are enabled except for tcp_syn_srcport_less_1024.</p> <p>action - When enabling DoS prevention, the following actions can be taken.</p> <ul style="list-style-type: none"> drop – Drop the attack packets. mirror – Mirror the packet to other port for further process. priority – Change packet priority by the Switch from 0 to 7. If the priority is not specified, the original priority will be used. rx_rate – controls the rate of the received DoS attack packets. If not specified, the default action is drop.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure a land attack and blat attack prevention:

```
DES-3200-28:4# config dos_prevention dos_type land_attack blat_attack state
enable action drop
Command: config dos_prevention dos_type land_attack blat_attack state enable
action drop

Success.

DES-3200-28:4#
```

enable dos_prevention trap_log	
Purpose	Used to enable a DoS prevention trap/log.
Syntax	enable dos_prevention trap_log
Description	This command is used to send traps and logs when a DoS attack event occurs. The event will be logged only when the action is specified as

enable dos_prevention trap_log

	drop.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable a DoS prevention trap/log:

```
DES-3200-28:4# enable dos_prevention trap_log
Command: enable dos_prevention trap_log

Success.

DES-3200-28:4#
```

disable dos_prevention trap_log

Purpose	Used to disable a DoS prevention trap/log.
Syntax	disable dos_prevention trap_log
Description	This command is used to disable a DoS prevention trap/log.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable a DoS prevention trap/log :

```
DES-3200-28:4# disable dos_prevention trap_log
Command: disable dos_prevention trap_log

Success.

DES-3200-28:4#
```

show dos_prevention	
Purpose	Used to display DoS prevention information.
Syntax	show dos_prevention { land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024 }
Description	This command is used to display DoS prevention information, including the type of DoS attack, the prevention state, the corresponding action if the prevention is enabled, and the counter information of the DoS packet.
Parameters	The type of DoS attack. Possible values are as follows: land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024
Restrictions	None.

Example usage

To display DoS prevention information:

```

DES-3200-28:4# show dos_prevention
Command: show dos_prevention
Trap/Log   : Enabled

DoS Type           State   Action           Frame Counts
Land Attack        Disabled Drop              0
Blat Attack        Enabled Drop             123
Smurf Attack       Enabled Mirror          1500
TCP Null Scan     Enabled Drop          100000
TCP Xmascan       Disabled Drop              0
TCP SYNFIN        Enabled Mirror        1245678
TCP SYN SrcPort Less Than 1024 Enabled Mirror        1234567890

DES-3200-28:4#
    
```


To display DoS prevention information for Land Attack:

```
DES-3200-28:4# show dos_prevention land_attack
Command: show dos_prevention land_attack

DoS Type: Land Attack
State: Enabled
Action: Mirror
    Port: 7
    Priority: 5
    Rx Rate(Kbit/sec): 1024
Frame Counts: 10000

DES-3200-28:4#
```

To display DoS prevention information for Blat Attack:

```
DES-3200-28:4# show dos_prevention blat_attack
Command: show dos_prevention blat_attack

DoS Type: Blat Attack
State: Enabled
Action: MirrorToPort
    Port: 7
    Priority: no_change
    Rx Rate(Kbit/sec): no_limit
Frame Counts: 10500

DES-3200-28:4#
```

clear dos_prevention counters

Purpose	Used to clear the counters of the prevention of each DoS attack.
Syntax	clear dos_prevention counters { land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024 }
Description	This command is used to clear the counters of the prevention of each DoS attack.
Parameters	The type of DoS attack. Possible values are as follows: land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024
Restrictions	Only Administrator-level users can issue this command.

Example usage

To clear all counters of the prevention of each DoS attack:

```
DES-3200-28:4# clear dos_prevention counters
Command: clear dos_prevention counters

Success.

DES-3200-28:4#
```

IP-MAC-PORT BINDING COMMANDS

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-port binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC-port binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC-port binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the Switch, the maximum value for the IP-MAC-port binding ARP mode is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

The IP-MAC-Port Binding commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> all]}
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> all]}
config address_binding ip_mac ports	[<portlist> all] {state [enable {[strict loose]} disable] allow_zeroip [enable disable] forward_dhcppt [enable disable] mode [arp acl] stop_learning_threshold <int 0-500>} (1)
show address_binding	{[ip_mac [all ipaddress <ipaddr> mac_address <macaddr>] blocked [all vlan_name <vlan_name> mac_address <macaddr>] ports]}
delete address_binding	[ip_mac [ipaddress <ipaddr> {mac_address <macaddr>} all] blocked [all vlan_name <vlan_name> mac_address <macaddr>]]
enable address_binding trap_log	
disable address_binding trap_log	
show address_binding dhcp_snoop	{[max_entry {ports <portlist>} binding_entry {port <port>}]}
enable address_binding dhcp_snoop	
disable address_binding dhcp_snoop	
clear address_binding dhcp_snoop binding_entry ports	[<portlist> all]
config address_binding dhcp_snoop max_entry ports	[<portlist> all] limit [<value 1-10> no_limit]
config address_binding recover_learning ports	[<portlist> all]
enable address_binding arp_inspection	
disable address_binding arp_inspection	

Each command is listed, in detail, in the following sections:

create address_binding ip_mac ipaddress

Purpose

Used to create an IP-MAC-port binding entry.

create address_binding ip_mac ipaddress

Syntax	create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> all]}
Description	This command is used to create an IP-MAC-port binding entry.
Parameters	<p><ipaddr> The IP address of the device where the IP-MAC-port binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC-port binding is made.</p> <p><portlist> - Specifies a port or range of ports to be configured for address binding.</p> <p>all – Specifies that all ports on the Switch will be configured for address binding.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DES-3200-28:4#create address_binding ip_mac ipaddress 10.1.1.3 mac_address
00-00-00-00-00-04
Command: create address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-
00-00-00-00-04

Success.

DES-3200-28:4#
```

config address_binding ip_mac ipaddress

Purpose	Used to configure an IP-MAC-port binding entry.
Syntax	config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> all]}
Description	This command is used to configure an IP-MAC-port binding entry.
Parameters	<p><ipaddr> - The IP address of the device where the IP-MAC-port binding is made.</p> <p><macaddr> - The MAC address of the device where the IP-MAC-port binding is made.</p> <p><portlist> - Specifies a port or range of ports to be configured for address binding.</p> <p>all – Specifies that all ports on the Switch will be configured for address binding.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3200-28:4#config address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-05
Command: config address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-05

Success.

DES-3200-28:4#
```

config address_binding ip_mac ports

Purpose	Used to configure an IP-MAC-port binding state to enable or disable for specified ports.
Syntax	config address_binding ip_mac ports [<portlist> all] {state [enable { [strict loose] } disable] allow_zeroip [enable disable] forward_dhcppt [enable disable] mode [arp acl] stop_learning_threshold <int 0-500>} (1)
Description	This command is used to configure the IP-MAC-port binding state to enable or disable for specified ports.
Parameters	<p><portlist> – Specifies a port or range of ports.</p> <p>all – Specifies all ports on the switch.</p> <p>state [enable disable] – Enables or disables the specified range of ports.</p> <p>strict - This mode provides a stricter control method. If a user chooses it, all packets will be sent to the CPU, thus all packets will not be forwarded by the hardware until the SW learns entries for the port. The port will check ARP packets and IP packets by IP-MAC-port binding entries. If a packet is found by the entry, the MAC address will be set to dynamic. If a packet is not found by the entry, the MAC address will be set to block. Other packets will be dropped. The default mode is strict if not specified.</p> <p>loose - This mode provides a more loose way of control. If a user chooses it, ARP packets and IP Broadcast packets will go to the CPU. The packet will still be forwarded by the hardware until a specific source MAC address is blocked by the software. The port will check ARP packets and IP Broadcast packets by IP-MAC-port binding entries. If a packet is found by the entry, the MAC address will be set to dynamic. If a packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed.</p> <p>allow_zeroip [enable disable] – Enables or disables zero IP address. When this function is enabled, the Switch doesn't block MAC which send ARP as sender protocol address with zero.</p> <p>forward_dhcppt [enable disable] – Enables or disables forward DHCP packet. By default, the DHCP packet with broadcast DA will be flooded. When set to disable, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP snooping is enabled, under which case the DHCP packet which has been trapped to the CPU needs to be forwarded by the software. This setting controls the forwarding behavior in this situation.</p> <p>mode [arp acl] – When configuring the mode of the port to ACL, the Switch will create an ACL access entry corresponding to the entries of this port. If the port changes to ARP, all the ACL access entries will be deleted automatically. The default mode of port is ARP mode.</p> <p>stop_learning_threshold <int 0-500> – When the number of blocked entries exceeds the threshold, the port will stop learning new addresses. The packet with new addresses will be dropped. The range is 0 to 500. The default is 500. Entering 0 means no limit.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3200-28:4#config address_binding ip_mac ports 2 state enable
Command: config address_binding ip_mac ports 2 state enable

Success.

DES-3200-28:4#
```

show address_binding	
Purpose	Used to display IP-MAC-port binding entries.
Syntax	show address_binding {[ip_mac [all ipaddress <ipaddr> mac_address <macaddr>] blocked [all vlan_name <vlan_name> mac_address <macaddr>] ports]}
Description	<p>This command is used to display IP-MAC-port binding entries. Three different kinds of information can be viewed.</p> <p>ip_mac – Address binding entries can be viewed by entering the physical and IP addresses of the device.</p> <p>blocked – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the physical address of the device.</p> <p>ports - The number of enabled ports on a device.</p>
Parameters	<p>ip_mac – The database the user creates for address binding.</p> <p>all – For IP MAC binding all specifies all the IP-MAC-port binding entries; for blocked address binding entries all specifies all the blocked VLANs and their bound physical addresses.</p> <p>blocked – The address database that the system auto learns and blocks.</p> <p><ipaddr> – The IP address of the device where the IP-MAC-port binding is made.</p> <p><macaddr> – The MAC address of the device where the IP-MAC-port binding is made.</p> <p><vlan_name> – The VLAN name the blocked MAC belongs to.</p>
Restrictions	None.

Example usage:

To display the global configuration of address binding on the Switch:

```
DES-3200-28:4#show address_binding
Command: show address_binding

Trap/Log           : Disabled
DHCP Snoop         : Disabled
ARP Inspection     : Disabled

DES-3200-28:4#
```

To display address binding entries on the Switch:

The ACL status will display HW ACL active or not. In ARP mode, all of the binding entries will be inactive. The HW ACL active entries will be effective on ACL mode ports.

```
DES-3200-28:4#show address_binding ip_mac all
Command: show address_binding ip_mac all
```

IP Address	MAC Address	Mode	ACL Status	Ports
10.1.1.1	00-00-00-00-00-11	Static	Active	1,3,5,7,8
10.1.1.2	00-00-00-00-00-12	Static	Active	1
10.1.1.10	00-00-00-00-00-aa	DHCP Snooping	Active	1

Total Entries : 3

```
DES-3200-28:4#
```

To display blocked address binding on the Switch:

```
DES-3200-28:4#show address_binding blocked all
Command: show address_binding blocked all
```

VID	VLAN Name	MAC Address	Port	Type
1	default	00-01-02-03-29-38	7	BlockByAddrBind
1	default	00-0C-6E-5C-67-F4	7	BlockByAddrBind
1	default	00-0C-F8-20-90-01	7	BlockByAddrBind
1	default	00-0E-35-C7-FA-3F	7	BlockByAddrBind
1	default	00-0E-A6-8F-72-EA	7	BlockByAddrBind

Total Entries : 5

```
DES-3200-28:4#
```

delete address_binding

Purpose	Used to delete IP-MAC-port binding entries.
Syntax	delete address_binding [ip_mac [ipaddress <ipaddr> {mac_address <macaddr>} all] blocked [all vlan_name <vlan_name> mac_address <macaddr>]]
Description	<p>This command is used to delete IP-MAC-port binding entries. Two different kinds of information can be deleted.</p> <p>ip_mac – Individual address binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to all will delete all the address binding entries.</p> <p>blocked – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the physical address of the device. To delete all the blocked address binding entries, toggle all.</p>
Parameters	<p><ipaddr> The IP address of the device where the IP-MAC-port binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC-port binding is made.</p> <p><vlan_name> The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.</p> <p>all – For IP-MAC-port binding all specifies all the IP-MAC-port binding entries; for blocked address binding entries all specifies all the blocked VLANs and their bound physical addresses.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an IP-MAC binding entry on the Switch:

```
DES-3200-28:4#delete address-binding ip-mac ipaddress 10.1.1.1
mac_address 00-00-00-00-00-06
Command: delete address-binding ip-mac ipaddress 10.1.1.1 mac_address 00-
00-00-00-00-06

Success.

DES-3200-28:4#
```


enable address_binding trap_log

Purpose	Used to enable the trap log for the IP-MAC-port binding function.
Syntax	enable address_binding trap_log
Description	This command, along with the disable address_binding trap_log will enable and disable the sending of trap log messages for IP-MAC-port binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the sending of IP-MAC-port binding trap log messages on the Switch:

```
DES-3200-28:4#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DES-3200-28:4#
```

disable address_binding trap_log

Purpose	Used to disable the trap log for the IP-MAC-port binding function.
Syntax	disable address_binding trap_log
Description	This command, along with the enable address_binding trap_log will enable and disable the sending of trap log messages for IP-MAC-port binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the sending of IP-MAC-port binding trap log messages on the Switch:

```
DES-3200-28:4#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DES-3200-28:
```

show address_binding dhcp_snoop

Purpose	To show address binding entries created by DHCP packet.
Syntax	show address_binding dhcp_snoop {[max_entry {ports <portlist>} binding_entry {port <port>}}}
Description	This command is used to show address binding DHCP snooping information.
Parameters	None.
Restrictions	None.

Example usage:

To display address binding DHCP snooping:

```
DES-3200-28:4#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP_Snoop : Enabled

DES-3200-28:4#
```

To display an address binding DHCP snooping entry:

```
DES-3200-28:4#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

IP Address      MAC Address      Lease Time (secs)  Port  Status
-----
10.1.1.1        00-00-00-00-00-11  1188               1     Active

Total Entries : 1

DES-3200-28:4#
```

To display address binding DHCP snooping maximum entry:

```
DES-3200-28:4#show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry

Port Max entry
-----
1      5
2      5
3      5
4      5
5      5
6      5
7      5
8      5
9      5
10     5
11     5
12     5
13     5
14     5
15     5
16     5
17     5
18     5
19     5
20     5
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Page A All
```

enable address_binding dhcp_snoop	
Purpose	Used to enable the address binding DHCP snooping.
Syntax	enable address_binding dhcp_snoop
Description	This command is used to enable the function to allow entries to be created by the DHCP packet. By default, DHCP snooping is disabled. If a user enables DHCP snooping, all address binding disabled ports will function as server ports (the Switch will learn IP addresses through server ports (by DHCP OFFER and DHCP ACK packets)).
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable address binding DHCP snooping:

```
DES-3200-28:4#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DES-3200-28:4#
```

disable address_binding dhcp_snoop

Purpose	Used to disable the address binding auto mode.
Syntax	disable address_binding dhcp_snoop
Description	This command is used to disable the function which allows entries to be created by the DHCP packet. When the DHCP snooping function is disabled, all of the auto-learned binding entries will be removed.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable address binding DHCP snooping:

```
DES-3200-28:4#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DES-3200-28:4#
```

clear address_binding dhcp_snoop binding_entry

Purpose	Used to clear the address binding entries learned for the specified ports.
Syntax	clear address_binding dhcp_snoop binding_entry ports [<portlist> all]
Description	This command is used to clear the address binding entries learned for the specified ports.
Parameters	ports - Specifies the list of ports that you would like to clear the dhcp-snoop learned entry.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To clear address binding DHCP snooping binding entries for ports 1 to 3:

```
DES-3200-28:4#clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DES-3200-28:4#
```

config address_binding dhcp_snoop max_entry

Purpose	Used to specify the maximum number of entries which can be learned by
----------------	---

config address_binding dhcp_snoop max_entry	
	the specified ports.
Syntax	config address_binding dhcp_snoop max_entry ports [<portlist> all] limit [<value 1-10> no_limit]
Description	This command is used to specify the maximum number of entries which can be learned by the specified ports. By default, the per port maximum entry is 5.
Parameters	<portlist> - Specifies the list of ports that you would like to set the maximum dhcp-snoop learned entry. limit - Specifies the maximum number.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To set the maximum number of entries that ports 1 to 3 can learn up to 10:

```
DES-3200-28:4#config address_binding dhcp_snoop max_entry ports 1-3 limit 10
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10

Success.

DES-3200-28:4#
```

config address_binding recover_learning ports	
Purpose	Used to unfreeze the learning of new addresses on a set of ports.
Syntax	config address_binding recover_learning ports [<portlist> all]
Description	This command is used to allow the Switch to learn new addresses again on ports which previously reached the stop learning threshold for blocked addresses.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable address binding DHCP snooping:

```
DES-3200-28:4#config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

DES-3200-28:4#
```

enable address_binding arp_inspection

Purpose	Used to enable ARP inspection.
Syntax	enable address_binding arp_inspection
Description	This command is used to filter ARP packets which have unauthorized sender MAC, IP address, and ingress port. ARP inspection is only active on IP-MAC-Port Binding enabled ports.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable ARP inspection:

```
DES-3200-28:4#enable address_binding arp_inspection
Command: enable address_binding arp_inspection

Success.

DES-3200-28:4#
```

disable address_binding arp_inspection

Purpose	Used to disable ARP inspection.
Syntax	disable address_binding arp_inspection
Description	This command is used to disable ARP inspection.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable ARP inspection:

```
DES-3200-28:4#disable address_binding arp_inspection
Command: disable address_binding arp_inspection

Success.

DES-3200-28:4#
```

LOOPBACK DETECTION COMMANDS

The Loopback Detection commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config loopdetect	{ recover_timer [0 <value 60-1000000>] interval < value 1-32767> mode [port-based vlan-based] } (1)
config loopdetect ports	[<portlist> all] state [enable disable]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[<portlist> all]
config loopdetect trap	[none loop_detected loop_cleared both]

Each command is listed, in detail, in the following sections:

config loopdetect

Purpose	Used to configure the loopback detection function on the Switch.
Syntax	config loopdetect { recover_timer [0 <value 60-1000000>] interval < value 1-32767> mode [port-based vlan-based] }(1)
Description	This command is used to set up the loopback detection function (LBD) for the entire Switch.
Parameters	<p>recover_timer - The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. Zero is a special value which means to disable the auto-recovery mechanism, hence, a user needs to recover the disabled port back manually. The default value of the recover timer is 60. The valid range is 60 to 1000000.</p> <p>interval - The time interval (in seconds) at which a device transmits all the CTP (Configuration Test Protocol) packets to detect the loopback event. The valid range is 1 to 32767. The default setting is 10.</p> <p>mode - Choose the loopback detection operation mode. In the port-based mode, the port will be shut-down (be disabled) when a loop is detected; in VLAN-based mode, the port cannot process packets on the VLAN on which the loop is detected. The default mode is port-based.</p> <ul style="list-style-type: none"> ▪ port-based – Specify the mode is port-based. A port-based loop refers to a loop caused by any port system wide. ▪ vlan-based – Specify the mode is VLAN-based. A VLAN-based loop refers to a loop within a VLAN detected on a member port of that VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set a recover time of 0 with an interval of 20 and VLAN-based mode:

```
DES-3200-28F:4# config loopdetect recover_timer 0 interval 20 mode vlan-
based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

DES-3200-28F:4#
```


config loopdetect ports

Purpose	Used to configure the loopback detection function for the port on the Switch.
Syntax	config loopdetect ports [<portlist> all] state [enable disable]
Description	This command is used to set up the loopback detection function for port configuration on the Switch.
Parameters	<portlist> – Specifies a range of ports to be configured for loopback detection status. all – Apply setting to all ports. state - Allows loopback detection to be enabled or disabled for the ports specified in the port list. The default is disabled. enable – Set port loopback detection status to enable. disable - Set port loopback detection status to disable.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To set the loopback detection status to enabled:

```
DES-3200-28F:4# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DES-3200-28F:4#
```

enable loopdetect

Purpose	Used to globally enable the loop-detect function on the Switch.
Syntax	enable loopdetect
Description	This command is used to allow the loop detection function to be globally enabled on the Switch. The default value is disabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage :

To enable loopback detection on the Switch:

```
DES-3200-28F:4# enable loopdetect
Command: enable loopdetect

Success.

DES-3200-28F:4#
```

disable loopdetect

Purpose	Used to globally disable the loopback detection on the Switch.
Syntax	disable loopdetect
Description	This command is used to globally disable the loopback detection on the Switch. The default value is disabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable the loopback detection function on the Switch:

```
DES-3200-28F:4# disable loopdetect
Command: disable loopdetect

DES-3200-28F:4#
```

show loopdetect

Purpose	Used to display the Switch's current loopback detection configuration.
Syntax	show loopdetect
Description	This command is used to display the Switch's current loopback detection configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the current loopback detection configuration on the Switch:

```
DES-3200-28F:4#show loopdetect
Command: show loopdetect

LBD Global Settings
-----
LBD Status           : Disabled
LBD Mode             : Port Based
LBD Interval         : 10
LBD Recover Time     : 60
LBD Trap Status      : None

DES-3200-28F:4#
```

show loopdetect ports

Purpose	Used to display the loopback detection configuration per port on the Switch.
Syntax	show loopdetect ports [<portlist> all]
Description	This command will display the Switch's current per-port loop-detect configuration and status.
Parameters	<portlist> – Specifies a range of ports to be configured. all – To set all the ports in the system, use the all parameter.
Restrictions	None.

Example usage:

To display loopback detection configuration of port 1-9 under port-based mode:

```
DES-3200-28:4#show loopdetect ports 1-9
Command: show loopdetect ports 1-9
```

Port	Loopdetect State	Loop Status
1	Enabled	Normal
2	Enabled	Normal
3	Enabled	Normal
4	Enabled	Loop
5	Enabled	Normal
6	Enabled	Normal
7	Enabled	Normal
8	Enabled	Normal
9	Enabled	Normal

config loopdetect trap

Purpose	Used to configure loopback detection traps.
Syntax	config loopdetect trap [none loop_detected loop_cleared both]
Description	This command is used to specify the trap modes for loop detection.
Parameters	none – A trap is not sent in either case. loop_detected - Trap is sent when the loop condition is detected. loop_cleared - Trap is sent when the loop condition is cleared. both – A trap is sent in either case.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set trap mode for loopback detection:

```
DES-3200-28F:4# config loopdetect trap both
Command: config loopdetect trap both

Success.

DES-3200-28F:4#
```

PROTOCOL VLAN COMMANDS

The Protocol VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
create dot1v_protocol_group	group_id <int 1-16> {group_name <name 32>}
config dot1v_protocol_group	[group_id <int 1-16> group_name <name 32>][add protocol [ethernet_2 ieee802.3_snap] <hex> delete protocol [ethernet_2 ieee802.3_snap] <hex>]
delete dot1v_protocol_group	[group_id <int 1-16> group_name <name 32> all]
show dot1v_protocol_group	{ [group_id <int 1-16> group_name <name 32>] }
config port dot1v ports	[all] [add protocol_group [group_id <int 1-16> group_name <name 32>] [vlan <vlan_name 32> vlanid <int>] { priority <value 0-7> } delete protocol_group [group_id <int 1-16> all]]
show port dot1v	{ports <portlist> }

Each command is listed, in detail, in the following sections:

create dot1v_protocol_group

Purpose	Used to create a protocol group for the protocol VLAN function.
Syntax	create dot1v_protocol_group group_id <int 1-16> {group_name <name 32>}
Description	This command is used to create a protocol group for the protocol VLAN function.
Parameters	<p>group_id - The ID of the protocol group which is used to identify a set of protocols.</p> <p>group_name - The name of the protocol group. The maximum length is 32 characters. If a group name is not specified, the group name will be automatically generated in accordance with ProtocolGroup+group_id. For example, the auto-generated name for group ID 2 is ProtocolGroup2. If the auto-generated name is in conflict with an existing group, an alternative name will be used in accordance with ProtocolGroup+group_id+ALT+num. The value for num starts with 1. If it is still in conflict, then subsequent number will be used instead. As an example: The auto-generated name for group ID 1 is "ProtocolGroup1". If this name already exists, then ProtocolGroup1ALT1 will be used instead.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a protocol group:

```
DES-3200-28:4# create dot1v_protocol_group group_id 1 group_name
General_Group
Command: create dot1v_protocol_group group_id 1 group_name General_Group

Success.

DES-3200-28:4#
```

config dot1v_protocol_group

Purpose	Used to add a protocol to a protocol group.
Syntax	config dot1v_protocol_group [group_id <int 1-16> group_name <name 32>][add protocol [ethernet_2 ieee802.3_snap] <hex> delete protocol [ethernet_2 ieee802.3_snap] <hex>]
Description	This command is used to add a protocol to a protocol group.
Parameters	<p>group_id – The ID of the protocol group which is used to identify a set of protocols.</p> <p>group_name – The name of the protocol group.</p> <p>protocol_value - The protocol value is used to identify a protocol of the frame type specified. Depending on the frame type, the octet string will have one of the following values: (The form of the input is 0x0 to 0xffff).</p> <p>For 'ethernet' II, this is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.</p> <p>For 'IEEE802.3 SNAP,' this is this is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a protocol IPv6 to protocol group 1:

```
DES-3200-28:4#config dot1v_protocol_group group_id 1 add protocol
Ethernet_2 0x86DD
Command: config dot1v_protocol_group group_id 1 add protocol Ethernet_2
0x86DD

The protocol value configured to add will take effect on both frame types
ethernet_2 and ieee802.3_snap.

Success.

DES-3200-28:4#
```

delete dot1v_protocol_group

Purpose	Used to delete a protocol from a protocol group.
Syntax	delete dot1v_protocol_group [group_id <int 1-16> group_name <name 32> all]
Description	This command is used to delete a protocol from a protocol group.
Parameters	<p>group_id – Specifies the group ID to be deleted.</p> <p>group_name – The name of the protocol group.</p> <p>protocol_value - The protocol value is used to identify a protocol of the frame type specified. Depending on the frame type, the octet string will have one of the following values: (The form of the input is 0x0 to 0xffff).</p> <p>For 'ethernet' II, this is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.</p> <p>For 'IEEE802.3 SNAP,' this is this is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete protocol group 1:

```
DES-3200-28:4# delete dot1v_protcol_group group_id 1
Command: delete dot1v_protcol_group group_id 1

Success.

DES-3200-28:4#
```


show dot1v_protocol_group

Purpose	Used to display the protocols defined in a protocol group.
Syntax	show dot1v_protocol_group {[group_id <int 1-16> group_name <name 32>}]
Description	This command is used to display the protocols defined in protocol groups.
Parameters	group_id – Specifies the group ID to be displayed. If a group ID is not specified, all configured protocol groups will be displayed. group_name – The name of the protocol group.
Restrictions	None.

Example usage:

To display the protocol group ID 1:

```
DES-3200-28:4# show dot1v_protocol_group group_id 1
Command: show dot1v_protocol_group group_id 1

Protocol Group ID Protocol Group Name          Frame Type      Protocol Value
-----
1                General_Group   EthernetII      86dd
1                General_Group   IEEE802.3 SNAP 86dd

Total Entries: 1
DES-3200-28:4#
```

config port dot1v ports	
Purpose	Used to assign the VLAN for untagged packets that ingress from the portlist based on the protocol group configured.
Syntax	config port dot1v ports [all] [add protocol_group [group_id <int 1-16> group_name <name 32>][vlan <vlan_name 32> vlanid <int>] {priority <value 0-7>} delete protocol_group [group_id <int 1-16> all]]
Description	This command is used to assign the VLAN for untagged packets that ingress from the portlist based on the protocol group configured. This assignment can be removed by using the delete protocol_group option. When priority is not specified in the command, the port default priority will be the priority for those untagged packets classified by the protocol VLAN.
Parameters	<p>all – Specifies that this command will apply to all ports.</p> <p>group_id – The group ID of the protocol group.</p> <p>group_name – The name of the protocol group.</p> <p>vlan – The VLAN that is to be associated with this protocol group on this port.</p> <p>vlan_id – Specifies the VLAN ID.</p> <p>priority – Specifies the priority to be associated with the packet which has been classified to the specified VLAN by the protocol.</p>
Restrictions	Only Administrator-level users can issue this command.



Note: For the current release of the DES-3200, users cannot specify a range of ports for 802.1v. The current release only allows users to specify all ports.

Example usage:

To assign VLAN marketing-1 for untagged IPv6 packet ingress from port 3 and to configure the group ID 100 on port 3 to be associated with VLAN marketing-1:

```
DES-3200-28:4# config port dot1v ports all add protocol_group group_id 1
vlan marketing-1
Command: config port dot1v ports all add protocol_group group_id 1 vlan
marketing-1

Success.

DES-3200-28:4#
```

show port dot1v

Purpose	Used to display the VLAN to be associated with untagged packets ingress from a port based on the protocol group.
Syntax	show port dot1v {ports <portlist> }
Description	This command is used to display the VLAN to be associated with untagged packets ingress from a port based on the protocol group.
Parameters	portlist – Specifies a range of ports to be displayed. If not specified, information for all ports will be displayed.
Restrictions	None.

Example usage:

To display protocol VLAN information for ports 1 to 2:

```
DES-3200-28:4# show port dot1v ports 1-2
Command: show port dot1v ports 1-2

Port: 1
Protocol Group ID      VLAN Name              Protocol Priority
-----
3                      default                -
4                      VLAN300                -
5                      marketing-1            -

Port: 2
Protocol Group ID      VLAN Name              Protocol Priority
-----
3                      default                -
4                      VLAN300                -
5                      marketing-1            -

Total Entries: 6
DES-3200-28:4#
```

MAC-BASED VLAN COMMANDS

The MAC-based VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
create mac_based_vlan	mac_address <macaddr> vlan <vlan_name 32>
delete mac_based_vlan	{mac_address <macaddr> vlan <vlan_name 32>}
show mac_based_vlan	{mac <macaddr> vlan <vlan_name 32>}

Each command is listed, in detail, in the following sections.

create mac_based_vlan

Purpose	Used to create a static MAC-based VLAN entry.
Syntax	create mac_based_vlan mac_address <macaddr> vlan <vlan_name 32>
Description	This command is used to create a static MAC-based VLAN entry. When a static MAC-based VLAN entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN regardless of the PVID operating on this port. There is a global limitation of the maximum entries supported for the static MAC-based entry.
Parameters	mac – The MAC address. vlan – The VLAN to be associated with the MAC address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a MAC-based VLAN local entry:

```
DES-3200-28:4# create mac_based_vlan mac_address 00:00:00:00:00:01 vlan
default
Command: create mac_based_vlan mac_address 00:00:00:00:00:01 vlan default

Success.

DES-3200-28:4#
```

delete mac_based_vlan

Purpose	Used to delete the static MAC-based VLAN entry.
Syntax	delete mac_based_vlan {mac_address <macaddr> vlan <vlan_name 32>}
Description	This command is used to delete a database entry. If the MAC address and VLAN are not specified, all static entries associated with the port will be removed.
Parameters	mac – The MAC address. vlan – The VLAN to be associated with the MAC address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a static MAC-based VLAN entry:

```
DES-3200-28:4# delete mac_based_vlan mac_address 00:00:00:00:00:01 vlan
default
Command: delete mac_based_vlan mac_address 00:00:00:00:00:01 vlan default

Success.

DES-3200-28:4#
```

show mac_based_vlan

Purpose	Used to display a static mac-based vlan entry.
Syntax	show mac_based_vlan {mac <macaddr> vlan <vlan_name 32>}
Description	This command is used to display a static MAC-Based VLAN entry.
Parameters	mac – The MAC address of the entry to display. vlan – The VLAN of the entry to display.
Restrictions	None.

Example usage:

In the following example, MAC address “00:80:c2:33:c3:45” is assigned to VLAN 300 by manual configuration. It is assigned to VLAN 400 by 802.1X. Since 802.1X has higher priority than manual configuration, the manual configured entry will become inactive.

To display the MAC-based VLAN entry:

```
DES-3200-28:4# show mac_based_vlan
Command: show mac_based_vlan

  MAC Address      VLAN    Status    Type
  -----
00-80-e0-14-a7-57  200     Active    Static
00-80-c2-33-c3-45  300     Inactive   Static
00-80-c2-c3-c3-45  400     Active    802.1X

Total Entries: 3

DES-3200-28:4#
```

FLOW METER COMMANDS

The Flow Meter commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config flow_meter profile_id	<value 1-512> access_id < access_id >[[rate <value 64-1024000> burst_size <value 0-1016> rate_exceed [drop_packet remark_dscp <value 0-63>]] delete]
show flow_meter	{profile_id <value 1-512> {access_id <access_id>}}

Each command is listed, in detail, in the following sections.

config flow_meter profile_id

Purpose	Used to configure packet flow-based metering based on an access profile and rule.
Syntax	config flow_meter profile_id <value 1-512> access_id < access_id >[[rate <value 64-1024000> burst_size <value 0-1016> rate_exceed [drop_packet remark_dscp <value 0-63>]] [delete]
Description	<p>This command is used to configure the flow-based metering function. The metering function supports only single-rate two-color mode. The access rule must first be created before the parameters of this function can be applied.</p> <p>Users may set the preferred bandwidth for the rule, in Kbps and once the bandwidth has been exceeded, overflow packets will be dropped or have its DSCP remarked, depending on user configuration.</p> <p>For packets conforming to the configured rate, the action will depend on whatever is configured in the ACL rule.</p> <p>Note that the metering will only apply if the ACL rule action is permit or mirror.</p>
Parameters	<p>profile_id – Specifies the profile ID.</p> <p>access_id – Specifies the access ID.</p> <p>flow_meter – Configure the one rate two colors flow meter.</p> <p>rate - This specifies the rate for the single rate two color mode. Specify the committed bandwidth in Kbps for the flow. The minimum rate is 64 Kbps and maximum rate which can be configured is 1024000. The effective rate however is in multiples of 62.5 Kbps. Therefore, configuring the rate to 100 Kbps will have an effective rate of 62.5Kbps</p> <p>burst_size - This specifies the burst size for the single rate two color mode. The unit is Kbytes. The minimum burst size is 0 Kbytes and the maximum is 1016 Kbytes. The effective burst size is in multiples of 8Kbytes. Therefore configuring burst size to 10 Kbytes will have an effective burst size of 8 Kbytes.</p> <p>rate_exceed - This specifies the action for packets which exceed the committed rate in the single rate two color mode. The action can be specified to be one of the following: drop_packet: The dropped packets. remark_dscp: Mark the packet with a specified DSCP. The packet will also be set to high drop precedence.</p> <p>delete – Delete the specified flow meter.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the rate and burst of incoming packets matching an ACL rule:

```
DES-3200-28:4# config flow_meter profile_id 1 access_id 1 rate burst_size 64 rate_exceed
drop_packet
Command: config flow_meter profile_id 1 access_id 1 rate burst_size 64 rate_exceed
drop_packet

Success.

DES-3200-28:4#
```


show flow_meter

Purpose	Used to display the flow-based metering configuration.
Syntax	show flow_meter {profile_id <value 1-512> {access_id <access_id>}}
Description	This command displays the flow meter configuration.
Parameters	profile_id – Specifies the profile ID. access_id – Specifies the access ID.
Restrictions	None.

Example usage:

To display the flow meter information:

```
DES-3200-28:4# show flow_meter
Command: show flow_meter

Flow Meter information:
-----
Profile ID : 1           Access ID : 1           Mode : Single-rate Two-color
Rate: 2000(Kbps)       Burst Size:1000(Kbyte)
Actions:
Conform : Permit
Violate : Drop

Profile ID : 1           Access ID : 2           Mode : Single-rate Two-color
Rate: 2000(Kbps)       Burst Size:1016(Kbyte)
Actions:
Conform : Permit
Violate : Permit       Replace_dscp : 20

Total Flow Meter Entries: 2
DES-3200-28:4#
```

MAC-BASED ACCESS CONTROL COMMANDS

The MAC-based Access Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
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 auth_failover	[enable disable]
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>] hold_time [infinite <sec 1-300>] max_users [no_limit <value 1-128>]} (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_mac	[ports [all <portlist>] mac_addr <macaddr>]
create mac_based_access_control_local mac	<macaddr> {[vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
config mac_based_access_control_local mac	<macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094> clear_vlan]
delete mac_based_access_control_local	[mac <macaddr> vlan <vlan_name 32> vlanid <vlanid 1-4094>]
show mac_based_access_control	{ 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	[no_limit <value 1-128>]
config mac_based_access_control authorization attributes	{ radius [enable disable] local [enable disable] } (1)
enable authorization attributes	
disable authorization attributes	
show authorization	
config mac_based_access_control trap state	[enable disable]
config mac_based_access_control log state	[enable disable]

Each command is listed, in detail, in the following sections:

enable mac_based_access_control

Purpose	Used to enable MAC-based access control.
Syntax	enable mac_based_access_control
Description	This command enables MAC-based access control on the Switch. By default this is not enabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the MAC-based access control globally on the Switch:

```
DES-3200-28F:4# enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DES-3200-28F:4#
```

disable mac_based_access_control

Purpose	Used to disable MAC-based access control.
Syntax	disable mac_based_access_control
Description	This will disable MAC-based access control on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable the MAC-based access control globally on the Switch:

```
DES-3200-28F:4# disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DES-3200-28F:4#
```

config mac_based_access_control password

Purpose	Used to configure the password of the MAC-based access control.
Syntax	config mac_based_access_control password <passwd 16>
Description	This command will set the password that will be used for authentication via RADIUS server.
Parameters	<password 16> - In RADIUS mode, the Switch communicates with the RADIUS server using this password. The maximum length of the key is 16.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the password for MAC-based access control:

```
DES-3200-28:4#config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

DES-3200-28:4#
```

config mac_based_access_control method

Purpose	Used to configure the MAC-based access control authenticating method.
Syntax	config mac_based_access_control method [local radius]
Description	This command specifies to authenticate via local database or via RADIUS server.
Parameters	local – Specify to authenticate via local database. radius – Specify to authenticate via RADIUS server.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the MAC-based access control method:

```
DES-3200-28:4#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DES-3200-28:4#
```

config mac_based_access_control auth_failover

Purpose	Used to configure MAC-based access control authentication failover.
Syntax	config mac_based_access_control auth_failover [enable disable]
Description	When the authentication failover is disabled, if RADIUS servers are unreachable, the authentication will fail. When the authentication failover is enabled, if RADIUS server authentication is unreachable, the local database will be used to do the authentication. By default, the state is disabled.
Parameters	enable – Enable the protocol authentication failover. disable – Disable the protocol authentication failover.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable MAC-based access control authentication failover:

```
DES-3200-28:4#config mac_based_access_control auth_failover enable
Command: config mac_based_access_control auth_failover enable

Success.

DES-3200-28:4#
```

config mac_based_access_control guest_vlan ports

Purpose	Used to configure MAC-based access control guest VLAN ports.
Syntax	config mac_based_access_control guest_vlan ports <portlist>
Description	This command is used configure MAC-based access control guest VLAN ports.
Parameters	portlist – The list of ports to be configured.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure MAC-based access control guest VLAN ports:

```
DES-3200-28:4#config mac_based_access_control guest_vlan ports 1-2
Command: config mac_based_access_control guest_vlan ports 1-2

Success.

DES-3200-28:4#
```

config mac_based_access_control ports

Purpose	Used to configure the parameters of the MAC-based access control.
Syntax	config mac_based_access_control ports [<portlist> all] {state [enable disable] mode [port_based host_based] aging_time [infinite <min 1-1440>] hold_time [infinite <sec 1-300>] max_users [no_limit <value 1-128>] } (1)
Description	<p>This command is used to configure the parameters of the MAC-based access control setting. When the MAC-AC function is enabled for a port, and the guest VLAN function for this port is disabled, the user attached to this port will not be forwarded unless the user pass the authentication. The user that does not pass the authentication will not be serviced by the Switch. If the user passes the authentication, the user will be able to forward traffic operated under the original VLAN configuration.</p> <p>When the MAC-AC function is enabled for a port, and the guest VLAN function for this port is enabled, it will move from the original VLAN member port, and become the member port of the guest VLAN. before the authentication process starts. After the authentication and authorization is enabled, if a valid VLAN is assigned by the RADIUS server, then this port will be removed from the guest VLAN and become the member port of the assigned VLAN.</p> <p>For guest VLAN mode, if the MAC address is authorized, but no VLAN information assigned from RADIUS Server or the VLAN assigned by RADIUS server is invalid (e.g. the assigned VLAN does not exist), this port/MAC will be removed from the member port of the guest VLAN and will become a member port of the original VLAN.</p>
Parameters	<p>ports - A range of ports that are enabled or disabled for the MAC-based access control function.</p> <p>state - Specify whether MAC AC function is enabled or disabled.</p> <p>mode – Either port-based or host-based. port_based means that all users connected to a port share the first authentication result. host_based means that each user can have its own authentication result.</p> <p>aging_time - A time period during which an authenticated host will be kept in an authenticated state. When the aging time is timed-out, the host will be moved back to an unauthenticated state.</p> <p>hold_time - If a host fails to pass the authentication, the next authentication will not start within the hold time unless the user clears the entry state manually.</p> <p>max_users - A threshold of maximum authorized client(s).</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a port state for MAC-based access control:

```
DES-3200-28:4#config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable

Success.

DES-3200-28:4#
```

create mac_based_access_control

Purpose	Used to assign the guest VLAN.
Syntax	create mac_based_access_control [guest_vlan <vlan_name 32>]

create mac_based_access_control

	guest_vlanid <vlanid 1-4094>]
Description	This command is used to assign the guest VLAN.
Parameters	guest_vlan – Specifies the name of the guest VLAN. guest_vlanid – Specifies the VLAN ID of the guest VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To create a MAC-based access control guest VLAN by guest VLAN ID:

```
DES-3200-28:4#create mac_based_access_control guest_vlanid 1
Command: create mac_based_access_control guest_vlanid 1

Success.

DES-3200-28:4#
```

delete mac_based_access_control

Purpose	Used to de-assign a guest VLAN.
Syntax	delete mac_based_access_control [guest_vlan <vlan_name 32> guest_vlanid <vlanid 1-4094>]
Description	This command is used to de-assign the guest VLAN. When the guest VLAN is de-assigned, the guest VLAN function is disabled.
Parameters	guest_vlan – Specifies the name of the guest VLAN. guest_vlanid – Specifies the VLAN ID of the guest VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To de-assign a guest VLAN:

```
DES-3200-28:4#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

DES-3200-28:4#
```

clear mac_based_access_control auth_mac

Purpose	Used to reset the current state of a user. The re-authentication will be started after the user traffic is received again.
Syntax	clear mac_based_access_control auth_mac [ports [all <portlist>] mac_addr <macaddr>]
Description	This command is used to clear the authentication state of a user (or

clear mac_based_access_control auth_mac

	port) . The port (or the user) will return to un-authenticated state. All the timers associated with the port (or the user) will be reset.
Parameters	ports – To specify the port range to delete MACs on them. <macaddr> – To delete a specified host with this MAC.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear the MAC being processed by MAC-based access control:

```
DES-3200-28:4#clear mac_based_access_control auth_mac ports all
Command: clear mac_based_access_control auth_mac ports all

Success.

DES-3200-28:4#
```

create mac_based_access_control_local mac

Purpose	Used to create the local database entry.
Syntax	create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
Description	This command is used to create the local database entry.
Parameters	mac – The MAC address that access accepts by local mode. vlan – If the MAC address is authorized, the port will be assigned to this VLAN. vlanid – If the MAC address is authorized, the port will be assigned to this VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a MAC-based access control local entry:

```
DES-3200-28:4#create mac_based_access_control_local mac 00-00-00-00-00-01
vlan default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default

Success.

DES-3200-28:4#
```

config mac_based_access_control_local mac

Purpose	Used to configure a MAC-based access control local database entry.
Syntax	config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094> clear_vlan]
Description	This command is used to configure a MAC-based access control local database entry previously created using the create mac_based_access_control_local command.
Parameters	mac - Specify the authenticated host's MAC address. vlan - Specify the target VLAN by VLAN name. When this host is authorized, the host is assigned to this VLAN.

config mac_based_access_control_local mac

vlanid - Specify the target VLAN by VID. When the host is authorized, it is assigned to this VLAN if the target VLAN exists.

clear_vlan - Clear target VLAN information for specific hosts from the local database.

Restrictions Only Administrator-level users can issue this command.

Example usage :

To configure the target VLAN “default” for the MAC-based Access Control local database entry 00-00-00-00-00-01:

```
DES-3200-28F:4# config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DES-3200-28F:4#
```

delete mac_based_access_control_local

Purpose Used to delete the local database entry.

Syntax delete mac_based_access_control_local [mac <macaddr> | [vlan <vlan_name 32> |
vlanid <vlanid 1-4094>]

Description This command is used to delete the local database entry.

Parameters mac – Delete database by this MAC address.

vlan – Delete database by this VLAN name.

vlanid – Delete database by this VLAN ID.

Restrictions Only Administrator-level users can issue this command.

Example usage

To delete a MAC-based access control local by MAC address:

```
DES-3200-28:4#delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DES-3200-28:4#
```

To delete a MAC-based access control local by VLAN name:

```
DES-3200-28:4#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

DES-3200-28:4#
```

show mac_based_access_control

Purpose Used to display the MAC-based access control setting.

Syntax show mac_based_access_control {ports {<portlist> } }

show mac_based_access_control

Description	This command is used to display the MAC-based access control setting.
Parameters	ports - Display the MAC-based access control port state.
Restrictions	None.

Example usage:

To display MAC-based access control:

```
DES-3200-28F:4#show mac_based_access_control
Command: show mac_based_access_control

MAC Based Access Control
-----
State                : Disabled
Method               : Local
Authentication Failover : Disabled
Password             : default
Max Users            : 128
Guest VLAN           : ----
Guest VLAN VID       : ----
Guest VLAN Member Ports : ----
Radius Authorization : Enabled
Local Authorization  : Enabled
Trap                 : Enabled
Log                  : Enabled

DES-3200-28F:4#
```

To display MAC-based access control ports:

```
DES-3200-28:4#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4

Port   State      Aging Time   Hold Time   Auth Mode   Max Users
-----
      (mins)      (secs)
-----
1      Enabled    100          100         Port_based  128
2      Enabled    100          200         Host_based  128
3      Enabled    50           300         Port_based  128
4      Enabled    200          100         Host_based  no limit

DES-3200-28:4#
```

show mac_based_access_control_local

Purpose	Used to display MAC-based access control local databases.
Syntax	show mac_based_access_control_local {[mac<macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
Description	This command is used to display MAC-based access control local databases.
Parameters	mac – Display MAC-based access control local databases by this MAC address. vlan – Display MAC-based access control local databases by the VLAN name.

show mac_based_access_control_local

vlanid – Display MAC-based access control local databases by the VLAN ID.

Restrictions None.

Example usage

To display MAC-based access control local databases:

```
DES-3200-28:4#show mac_based_access_control_local
Command: show mac_based_access_control_local

  MAC Address          VLAN Name          VID
  -----
00-00-00-00-00-01    default            1
00-00-00-00-00-02    v123               123
00-00-00-00-00-03    v123               123
00-00-00-00-00-04    default            1

Total Entries: 4

DES-3200-28:4#
```

To display MAC-based access control local databases by MAC address:

```
DES-3200-28:4#show mac_based_access_control_local mac 00-00-00-00-00-01
Command: show mac_based_access_control_local mac 00-00-00-00-00-01

  MAC Address          VLAN Name          VID
  -----
00-00-00-00-00-01    default            1

Total Entries: 1

DES-3200-28:4#
```

To display MAC-based access control local databases by VLAN:

```
DES-3200-28:4#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address          VLAN Name          VID
-----
00-00-00-00-00-01   default           1
00-00-00-00-00-04   default           1

Total Entries: 2

DES-3200-28:4#
```

show mac_based_access_control_auth_state

Purpose	Used to display the MAC-based access control authentication state.
Syntax	show mac_based_access_control_auth_state {ports <portlist>}
Description	This command is used to display the MAC-based access control authentication state.
Parameters	ports – Display authentication status by port.
Restrictions	None.

Example usage:

MAC 00-00-00-00-00-01 is authenticated without a VLAN assigned (the specified target VLAN might not exist or a target VLAN has not been specified). The ID of RX VLAN will be displayed (the RX VLAN ID is 4004 in this example).

MAC 00-00-00-00-00-02 is authenticated with a target VLAN assigned. The ID of the target VLAN will be displayed (target VLAN ID is 1234 in this example).

MAC 00-00-00-00-00-03 failed to pass authentication, and packets with SA 00-00-00-00-00-03 will be dropped no matter which VLAN these packets are from.

To display the MAC-based access control authentication state:

```
DES-3200-28:4#show mac_based_access_control_auth_state
Command: show mac_based_access_control_auth_state

(P):Port based
Port    MAC Address          Auth State    VID    Priority    Aging Time/Hold Time
-----
1       00-00-00-00-00-01   Authenticated 4004    3          Infinite
2       00-00-00-00-00-02   Authenticated 1234    -          Infinite
3       00-00-00-00-00-03   Blocked       1       -          60
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

config mac_based_access_control_max_users

Purpose	Used to configure the maximum number of authorized clients.
Syntax	config mac_based_access_control_max_users [no_limit <value 1-128>]

config mac_based_access_control max_users

Description	This command is used to specify the maximum user limit per counter.
Parameters	<code>no_limit</code> – Specify to not limit the system maximum user number. <code><value 1-128></code> – Specify to set the maximum number of authorized clients on the whole device.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the MAC-based access control maximum number of users:

```
DES-3200-28:4#config mac_based_access_control max_users 128
Command: config mac_based_access_control max_users 128

Success.

DES-3200-28:4#
```

config mac_based_access_control authorization attributes

Purpose	Used to enable or disable local or RADIUS authorization to accept an authorized configuration.
Syntax	config mac_based_access_control authorization attributes { radius [enable disable] local [enable disable] } (1)
Description	<p>Used to enable or disable an authorized configuration to be accepted.</p> <p>When authorization is enabled for MAC-based access controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted if the global authorization status is enabled.</p> <p>When authorization is enabled for MAC-based access controls with local authentication, the authorized attributes assigned by the local database will be accepted.</p>
Parameters	<p>radius - If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted when the global authorization status is enabled with the enable authorization attributes command.</p> <p>The default state is enabled.</p> <p>local - If specified to enable, the authorized attributes assigned by the local database will be accepted if the global authorization status is enabled with the enable authorization attributes command.</p> <p>The default state is enabled.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

The following example will disable the configuration authorized from the local database:

```
DES-3200-28F:4# config mac_based_access_control authorization attributes local
disable
Command: config mac_based_access_control authorization attributes local disable

Success.

DES-3200-28F:4#
```

enable authorization attributes

Purpose	The enable authorization command globally enables the authorization for attributes function.
Syntax	enable authorization attributes
Description	Used to enable authorization attributes. When enabled, authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server or local database. Which attributes will be accepted depends on the individual module's setting. Authorization for attributes is disabled by default.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

This example sets authorization global state to enabled:

```
DES-3200-28F:4# enable authorization attributes
Command: enable authorization attributes

Success.

DES-3200-28F:4#
```

disable authorization attributes

Purpose	The disable authorization attributes command globally disables the authorization attributes function.
Syntax	disable authorization attributes
Description	Used to disable authorization attributes. When the authorization for attributes is disabled, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server or local database will be ignored even if the individual module's setting is enabled. Authorization for attributes is disabled by default.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

This example sets authorization global state disabled:

```
DES-3200-28F:4# disable authorization attributes
Command: disable authorization attributes

Success.

DES-3200-28F:4#
```

show authorization

Purpose	Used to display authorization for attributes status.
Syntax	show authorization
Description	Used this to view authorization for attributes status.
Parameters	None.
Restrictions	None.

Example usage:

This example displays authorization status:

```
DES-3200-28F:4# show authorization
Command: show authorization

Authorization for Attributes: Enabled

DES-3200-28F:4#
```

config mac_based_access_control trap state

Purpose	Used to enable or disable sending of MAC-based Access Control traps.
Syntax	config mac_based_access_control trap state [enable disable]
Description	When MAC-based Access Control trap state is enabled, The trap of MAC-based Access Control will be sent out. If the MAC-based Access Control trap state is disabled, no trap will be sent out.
Parameters	enable – To enable sending MAC-based Access Control traps. disable – To disable sending MAC-based Access Control traps.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable trap state of MAC-based Access Control:

```
DES-3200-28F:4# config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

DES-3200-28F:4#
```


config mac_based_access_control log state

Purpose	Used to enable or disable generating of MAC-based access control logs.
Syntax	config mac_based_access_control log state [enable disable]
Description	When MAC-based access control log state is enabled, The log of MAC-based access control will be generated. If the MAC-based access control log state is disabled, no log will be generated.
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-level users can issue this command.

Example usage:

To disable log state of MAC-based Access Control:

```
DES-3200-28F:4# config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable
Success.

DES-3200-28F:4#
```

ARP SPOOFING PREVENTION COMMANDS

The ARP Spoofing Prevention commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

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

Each command is listed, in detail, in the following sections:

config arp_spoofing_prevention

Purpose	Used to configure the prevention of ARP spoofing attacks.
Syntax	config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> all] delete gateway_ip <ipaddr>]
Description	This command is used to configure the prevention of ARP spoofing attacks. Configure the spoofing prevention entry to prevent spoofing of MAC for the protected gateway. When an entry is created, those ARP packets whose sender IP matches the gateway IP of an entry but either its sender MAC field or source MAC field does not match the gateway MAC of the entry, will be dropped by the system.
Parameters	<p>add gateway_ip – Specify a gateway IP to be configured.</p> <p>add gateway_mac – Specify a gateway MAC to be configured.</p> <p><portlist> – Specify a range of ports to be configured.</p> <p>all – Specifies all of the ports will be configured.</p> <p>delete gateway_ip – Specify a gateway IP to be configured.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure ARP spoofing prevention:

```
DES-3200-28:4#config arp_spoofing_prevention add gateway_ip 10.254.254.251
gateway_mac 00-00-00-11-11-11 ports 1-2
Command: config arp_spoofing_prevention add gateway_ip 10.254.254.251
gateway_mac 00-00-00-11-11-11 ports 1-2

Success.
DES-3200-28:4#
```

show arp_spoofing_prevention

Purpose	Used to display ARP spoofing prevention entries.
Syntax	show arp_spoofing_prevention
Description	This command is used to display ARP spoofing prevention entries.
Parameters	None.
Restrictions	None.

Example usage:

To display the current ARP spoofing prevention entry/entries:

```
DES-3200-28:4#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-3200-28:4#
```

TECHNICAL SUPPORT COMMANDS

The Technical Support commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
show tech_support	
upload tech_support_toTFTP	<ipaddr> <path_filename 64>

Each command is listed, in detail, in the following sections:

show tech_support	
Purpose	Used to show the information for technical support.
Syntax	show tech_support
Description	This command is especially used by the technical support personnel to dump the device's overall operation information. The information is project dependent and includes the following information. Basic System information system log Running configuration Layer 1 information Layer 2 information Layer 3 information Application OS status
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display technical support information on the Switch:

```

DES-3200-28:4#show tech_support
Command: show tech_support

                               DES-3200-28 Fast Ethernet Switch
                               Technical Information Report
=====
[CPU Utilization 8292070ms]
CPU Utilization :
-----
Five Seconds -   1 %           One Minute -   3 %           Five Minutes -  6 %

[Device Information 8292270ms]
Device Type       : DES-3200-28 Fast Ethernet Switch
MAC Address       : 00-00-01-02-03-04
IP Address        : 10.90.90.90 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.006
Firmware Version  : Build 1.28.005
Hardware Version  : B1
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
802.1x           : Disabled
TELNET            : Enabled(TCP 23)
WEB               : Enabled(TCP 80)
RMON              : Disabled
SSH               : Disabled
SSL               : Disabled
Syslog Global State: Disabled
Dual Image        : Supported
Password Encryption Status : Disabled

[Connection Session Status 8292470ms]
ID   Login Time      Live Time      From           Level   Name
--   -
8    0/00/00 01:30:41    0:47:30.90   Serial Port    4       Anonymous

Total Entries: 1

[Port Status 8292670ms]
Port   State/          Settings          Connection          Address
      MDI          Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
-----
1     Enabled      100M/Full/Disabled  LinkDown             Enabled
2     Enabled      100M/Full/Disabled  LinkDown             Enabled
3     Enabled      100M/Full/Disabled  LinkDown             Enabled
. . .

```

upload tech_support_toTFTP

Purpose	Used to upload information for assistance from technical support.
Syntax	upload tech_support_toTFTP <ipaddr> <path_filename 64>
Description	This command is used to upload information for assistance from technical support to a TFTP server.
Parameters	ipaddr – Specifies the IP address of the TFTP server. path_filename – Specifies the file path to use to send information for technical support to a TFTP server.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To upload Switch information for technical support:

```
DES-3200-28:4#upload tech_support_toTFTP 10.55.47.1
tech_support_20090521.txt
Command: upload tech_support_toTFTP 10.55.47.1 tech_support_20090521.txt

Connecting to server.....Done.
Upload technical support information.. Done.

Success.

DES-3200-28:4#
```

COMMAND HISTORY COMMANDS

The Command History commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
?	
dir	
config command_history	<value 1-40>
show command_history	

Each command is listed, in detail, in the following sections:

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	? {<command>}
Description	This command is used to display all of the commands available through the Command Line Interface (CLI).
Parameters	{<command>} – Entering the question mark with an appropriate command will list all the corresponding parameters for the specified command, along with a brief description of the commands function and similar commands having the same words in the command.
Restrictions	None.

Example usage

To display all of the commands in the CLI:


```

DES-3200-28:4#?
..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear dos_prevention counters
clear fdb
clear igmp_snooping data_driven_group
clear log
Clear mac_based_access_control auth_mac
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
    
```

To display the parameters for a specific command:

```

DES-3200-28:4#? config account
Command:? config account

Command: config account
Usage: <username>{encrypt [plain_text| sha_1] <password>}
Description: config user account

DES-3200-28:4#
    
```

dir

Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	dir
Description	This command is used to display all of the commands available through the Command Line Interface (CLI).
Parameters	None.
Restrictions	None.

Example usage:

To display all commands:

```
DES-3200-28:4#dir
..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear dos_prevention counters
clear fdb
clear igmp_snooping data_driven_group
clear log
clear mac_based_access_control auth_mac
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config command_history

Purpose	Used to configure the command history.
Syntax	config command_history <value 1-40>
Description	This command is used to configure the command history.
Parameters	<value 1-40> – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the command history:

```
DES-3200-28:4#config command_history 20
Command: config command_history 20

Success.

DES-3200-28:4#
```

show command_history

Purpose	Used to display the command history.
Syntax	show command_history
Description	This command is used to display the command history.
Parameters	None.
Restrictions	None.

Example usage

To display the command history:

```
DES-3200-28:4#show command_history
Command: show command_history

?
? show
show vlan
show command history

DES-3200-28:4#
```

CONNECTIVITY FAULT MANAGEMENT COMMANDS

Connectivity Fault Management (CFM) or Ethernet Connectivity Fault Management is an end-to-end Ethernet layer OAM protocol. CFM is defined by IEEE 802.1ag and includes connectivity monitoring, fault notification and means of isolating faults on large Ethernet metropolitan-area networks (MANs) and WANs.

Ethernet has traditionally operated on isolated enterprise LANs. As Ethernet has been expanded to operate on the much larger scale carrier networks that encompass multiple administrative domains, the demands of the much larger and more complex networks required a new set of OAM capabilities. Since these larger scale networks have a very large user base, carry more diversified network applications and typically span a much larger geographical area than traditional enterprise Ethernet LANs where link uptime is crucial, a means of dealing with connectivity faults able to operate in Ethernet became necessary. Since none of the existing OAM protocols could adequately address this new circumstance, Ethernet Connectivity Fault Management has been developed in order to meet the new operational management needs created by the application of Ethernet technologies to MANs and WANs.

Ethernet CFM provides Ethernet network service providers with various benefits such as end-to-end service-level OAM and lower operating expenses, all operated on top of a familiar Ethernet platform.

CFM introduces some new terms and concepts to Ethernet, these are briefly described below.

Maintenance Domain

A maintenance domain is generic term referring to a management area created for the purpose of managing and administering a network. A maintenance domain is operated by a single entity or “owner” and defined by a boundary with a set of ports internal to this boundary.

An Ethernet CFM maintenance domain, referred to in this manual simply as an MD, exists in a hierarchical relationship to other MDs. Typically a large MAN or WAN can be partitioned into a hierarchy based on the size of domain that mirrors the structural relationship of customers, service providers and operators. The service providers have end-to-end service responsibility while operators provide service transport across subnetworks. The hierarchy is defined by a maintenance level value ranging from 0 to 7 where 7 is the highest level and 0 the lowest level. The larger the MD is, the higher its maintenance level will be. For example, if the customer domain is the largest MD, it should be assigned a maintenance level of 7, the operator MD being the smallest, receives a maintenance level of 0 with the service provider domain being in between these values. Maintenance levels are manually assigned by the network administrator. All levels of the MD hierarchy must operate together.

Nesting of MDs is allowed, however they cannot intersect since this violates the requirement that management of MDs be done by a single owner. If two or more domains are nested, the outer domain must be assigned a higher maintenance level than the nested domains.

CFM operations and message exchanges are conducted on a per-domain basis. This means for example, that CFM operating at level 3 does not allow discovery of the level 3 network by higher levels.

Maintenance Association

A maintenance association (MA) in CFM is a set of MEPs that have been configured with the same management domain level and maintenance association identifier (MAID).

Different MAs in an MD must have different MA Names. Different MAs in different MDs may have the same MA Name. The MEP list specified for a MA can be located in different devices. MEPs must be created on ports of these devices explicitly. A MEP will transmit CCM packets periodically across the MA. The receiving MEP will verify these received CCM packets from other MEPs against this MEP list for configuration integrity check.

Maintenance Point

A maintenance point in CFM is a point of demarcation on a port within a maintenance domain. Maintenance points filter CFM frames within the boundaries of an MD by dropping frames that do not belong to the correct maintenance level. There are two types of maintenance points, **Maintenance Endpoints** (MEPs) and **Maintenance Intermediate Points** (MIPs). MEPS and MIP are manually configured by a network administrator.

A MEP exists at the edge of a maintenance domain, defining the boundary of the MD. MEP functions include filtering CFM messages so that they are confined to the MD. A MEP can be configured to transmit Connectivity Check Messages (CCMs) and will transmit treacroute and loopback messages if configured to do so. A MEP can be *Inward* facing or *Outward* facing.

An Inward facing MEP source CFM frames toward the bridge relay function, not through the bridge port on which the MEP is configured. An Inward facing MEP drops all CFM frames at its level or lower that are received from the Inward side; and forwards all CFM frames at a higher level regardless of the origin of the frame, Inward or Outward. If the port on which the inward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can no longer transmit or receive CFM messages.

An Outward facing MEP source frames toward the bridge port and can only be configured on routed ports. An Outward facing port drops all CFM frames at its level or lower coming from the bridge relay function side. It processes all CFM frames at its level, and drops all CFM frames at a lower level, coming from the bridge port. An Outward facing port forwards all CFM frames at

higher levels regardless of which direction the frames come in. If the port on which the outward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can still transmit and receive CFM messages through the bridge port.

A MIP is a maintenance point that is internal to an MD, not at the boundary. A MIP receives CFM frames from other MIPs and from MEPs. These frames are cataloged and forwarded using the bridge relay function and bridge port. All CFM frames at a lower level than the MIP are blocked and dropped regardless of the origin. All CFM frames at a higher level are forwarded regardless of the origin. If the port on which a MIP is configured is blocked by Spanning-Tree Protocol, the MIP cannot receive CFM messages or relay them toward the bridge relay function side. The MIP can, however, receive and respond to CFM messages from the bridge port.

CFM messages include Continuity Check Messages (CCMs), Loopback Messages (LBMs) and Link Trace Messages (LTMs). CFM uses standard Ethernet frames that can be sourced, terminated, processed and relayed by bridges. Routers support limited CFM functions.

Continuity Check Messages (CCMs) are multicast messages exchanged among MEPs. CCMs allow discovery of MEPs for other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a maintenance domain. CCMs are cataloged by MIPs are the same maintenance level and terminated by remote MEPs at the same maintenance level. They are unidirectional (no response solicitation) and carry the status of the port on which the MEP is configured. LBMs are similar to Ping or ICMP messages in that they indicate only whether a destination is reachable and do not allow discovery of each hop.

Link Trace Messages (LTMs) are multicast CFM frames sent by MEPs to identify adjacency relationships with remote MEPs and MIPs at the same maintenance level. The message body of an LTM includes a destination MAC address of a target MEP that terminates the linktrace. When a MIP or MEP receives an LTM, it generates a unicast Link Trace Reply (LTR) to the initiating MEP. It also forwards the LTM to the target MEP destination MAC address. An LTM effectively traces the path to the target MEP or MIP.

Loopback Messages (LBMs) are similar to Ping or ICMP messages in that they indicate only whether a destination is reachable and do not allow the discovery of each hop.

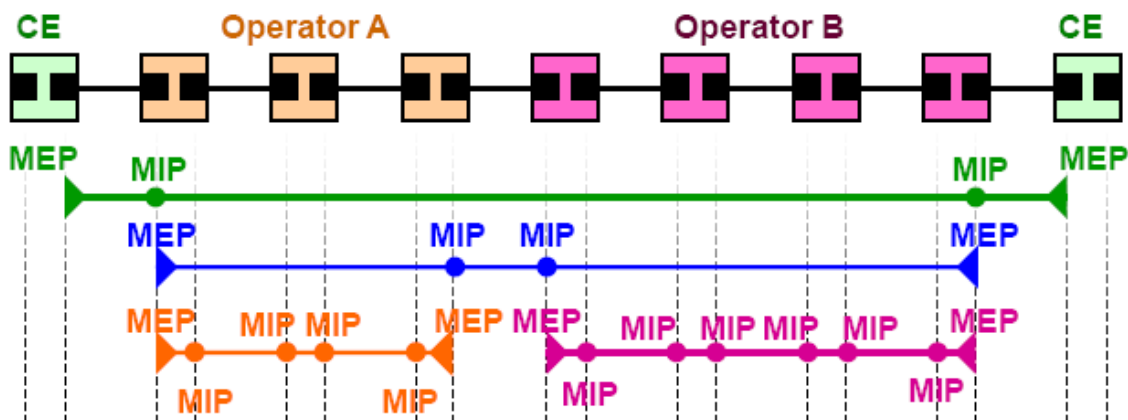


Figure 3 - 1. OAM Domain Architecture

- Maintenance Association (MA) – Boundaries of an Administrator’s scope of monitoring part of the network
- Maintenance Domain (MD) – A level of monitoring within the hierarchy
- Maintenance End Points (MEP) – End Points of the MA or MD
- Maintenance Intermediate Points (MIP) – Intermediate Points within MA or MD

Note: CE = Customer Equipment

The Connectivity Fault Management (CFM) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create cfm md	<string 22> level <int 0-7>
config cfm md	<string 22> { mip [none auto explicit] sender_id [none chassis manage chassis_manage] } (1)
create cfm ma	<string 22> md <string 22>
config cfm ma	<string 22> md <string 22> { 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> }(1)
create cfm mep	<string 32> mepid <int 1-8191> md <string 22> ma <string 22> direction [inward outward] port <port>
config cfm mep	[mepname <string 32> mepid <int 1-8191> md <string 22> ma <string 22>] {state [enable disable] ccm [enable disable] pdu_priority <int 0-7> fault_alarm [all mac_status remote_ccm error_ccm xcon_ccm none] alarm_time < centisecond 250-1000> alarm_reset_time < centisecond 250-1000>}(1)
delete cfm mep	[mepname <string 32> mepid <int 1-8191> md <string 22> ma <string 22>]
delete cfm ma	<string 22> md <string 22>
delete cfm md	<string 22>
enable cfm	
disable cfm	
config cfm ports	<portlist> state [enable disable]
show cfm ports	<portlist>
show cfm	{ [md <string 22> { ma <string 22> { mepid <int 1-8191> } } mepname <string 32>] }
show cfm fault	{ md <string 22> { ma <string 22> } }
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> ma <string 22>] {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> ma <string 22>] {ttl <int 2-255> pdu_priority <int 0-7>}
show cfm linktrace	[mepname <string 32> mepid <int 1-8191> md <string 22> ma <string 22>] { trans_id <uint> }
delete cfm linktrace	{ [md <string 22> { ma <string 22> { 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	[md <string 22> ma <string 22> mepid <int 1-8191> mepname <string 32>] 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] }

Each command is listed, in detail, in the following sections:

create cfm md

Purpose	Used to create a maintenance domain for CFM.
Syntax	create cfm md <string 22> level <int 0-7>
Description	Use this command to create a CFM maintenance domain and set the level for that domain.
Parameters	md <string 22> - The new CFM maintenance domain name, each domain should have a unique name. level <int 0-7> - The level of the CFM domain. Level 7 is the highest level and 0 is the lowest.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a maintenance domain called “op_domain” and assign a maintenance domain level of “2”:

```
DES-3200-28F:4# create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

DES-3200-28F:4#
```

config cfm md

Purpose	Used to configure the parameters of a previously created CFM maintenance domain.
Syntax	config cfm md <string 22> { mip [none auto explicit] sender_id [none chassis manage chassis_manage] } (1)
Description	Use this command for the creation of maintenance intermediate points (MIP) on the Maintenance Association (MA) of the specified Maintenance Domain (MD). This is useful to trace the link, MIP by MIP. It also allows the user to perform a loopback from a CFM maintenance endpoint (MEP) to an MIP.
Parameters	md <string 22> - The name of the previously created maintenance domain (MD). mip - This will create a maintenance intermediate points (MIP). none - No MIP is created. This is the default value. auto – MIPs on the MA of the specified MD can be created on any port in the MD, if the port is not configured with an MEP of the MD being configured. For an intermediate switch with the same Maintenance Administration (MA) configuration of the specific Maintenance Domain (MD), the setting can be automatic for convenient use compared with the following "explicit" setting. explicit - MIPs can only be created on a port which has an existing lower level MEP configured on it AND that port is not configured with an MEP of this MD. sender_id - This is the control transmission of the sender identifier (ID) Type Length Value (TLV). none - No sender ID TLV is transmitted. 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-level users can issue this command.

Example usage

To configure the maintenance domain called “op_domain” and specify the explicit option for creating MIPs:

```
DES-3200-28F:4# config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DES-3200-28F:4#
```

create cfm ma

Purpose	Used to create a maintenance association.
Syntax	create cfm ma <string 22> md <string 22>
Description	Each MA in an MD must have a name unique within the MD. Names of MA can be duplicated as long as they are not within the same MD.
Parameters	ma <string 22> - The name of the new maintenance association (MA). md <string 22> - The name of the previously created maintenance domain (MD) with which the MD is to be associated.
Restrictions	Only Administrator-level users can issue this command.

Example usage :

To create a maintenance association called “op1” and assign it to the maintenance domain “op_domain”:

```
DES-3200-28F:4# create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DES-3200-28F:4#
```


config cfm ma	
Purpose	This command is used to configure the parameters of a previously created CFM maintenance association.
Syntax	config cfm ma <string 22> md <string 22> { 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> }(1)
Description	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 Continuity Check Message (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.
Parameters	<p>ma <string 22> - The name of the previously created maintenance association (MA).</p> <p>md <string 22> - The name of the previously created maintenance domain (MD).</p> <p>Vlanid – The VLAN Identifier. There cannot be any overlap of MAs and associated VLANs, that is, each VLAN can associate with only one MA.</p> <p>mip - This will create a maintenance intermediate points (MIP).</p> <p>none - No MIP is created. This is the default value.</p> <p>auto - MIPs can be created on any port in the MD, if the port is not configured with an MEP of the MD being configured.</p> <p>For an intermediate switch in a maintenance administration (MA), the setting must be automatic in order for the MIPs to be created on this device.</p> <p>explicit - MIPs can only be created on a port which has an existing lower level MEP configured on it AND that port is not configured with an MEP of this MD.</p> <p>defer – The settings of the associated MD are inherited and applied to the MA. This is the default value.</p> <p>sender_id - This is the control transmission of the sender identifier (ID) Type Length Value (TLV).</p> <p>none - No sender ID TLV is transmitted. This is the default value.</p> <p>chassis - Transmit the sender ID TLV with the chassis ID information.</p> <p>manage - Transmit the sender ID TLV with the managed address information.</p> <p>chassis_manage - Transmit sender ID TLV with chassis ID information and manage address information.</p> <p>defer – The settings of the associated MD are inherited and applied to the MA. This is the default value.</p> <p>ccm_interval This is the CCM interval, use one of the predefined values: 10ms: 10 milliseconds. Not recommended. For test purposes. 100ms: 100 milliseconds. Not recommended. For test purposes. 1sec: One second. 10sec: Ten seconds. This is the default value. 1min: One minute. 10min: Ten minutes.</p> <p>mepid <mepid_list> This is to specify the MEP identifiers contained in the maintenance association. The range of the MEPID is 1-8191.</p> <p>add - Add MEPID(s).</p> <p>delete - Delete MEPID(s).</p> <p>By default, there is no MEPID in a newly created maintenance association.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure parameters for MA “op1”:

```
DES-3200-28F:4# config cfm ma op1 md op_domain vlan 1 ccm_interval 1sec
Command: config cfm ma op1 md op_domain vlan 1 ccm_interval 1sec

Success.

DES-3200-28F:4#
```

create cfm mep

Purpose	This command is used to create an MEP.
Syntax	create cfm mep <string 32> mepid <int 1-8191> md <string 22> ma <string 22> direction [inward outward] port <port>
Description	<p>Each MEP in an MA must have an MEPID unique within the MA. Each MEP in an individual Switch must also have a name unique within the MA. The MD name, MA name, and MEPID are used together to identify an MEP.</p> <p>Before creating an MEP, its MEPID should be configured in the MA’s MEPID list using the config cfm ma command described above.</p>
Parameters	<p>mep <string 32> - MEP name. It is unique among all MEPs configured on the device.</p> <p>mepid <int 1-8191> - This is to specify the MEP identifiers contained in the maintenance association. This must first be created with the config cfm ma command, mepid_list [add delete] <mepid_list> option.</p> <p>ma <string 22> - The name of the previously created maintenance association (MA).</p> <p>md <string 22> - The name of the previously created maintenance domain (MD).</p> <p>direction – The direction of the MEP.</p> <p>inward - Inward facing (up) MEP. An Inward facing MEP source CFM frames through the bridge relay function, not through the wire on which the MEP is configured. An Inward facing MEP drops all CFM frames at its level or lower that are received from the Inward side; and forwards all CFM frames at a higher level regardless of the origin of the frame, Inward or Outward. If the port on which the inward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can no longer transmit or receive CFM messages.</p> <p>outward - Outward facing (down) MEP. An Outward facing MEP source frames toward the wire and can only be configured on routed ports. An Outward facing port drops all CFM frames at its level or lower coming from the bridge relay function side. It processes all CFM frames at its level, and drops all CFM frames at a lower level, coming from the wire. An Outward facing port forwards all CFM frames at higher levels regardless of which direction the frames come in. If the port on which the outward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can still transmit and receive CFM messages through the wire.</p> <p>port <port> - Switch port number. The port must be a member of the VLAN associated with the MA.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a MEP named “mep1”:

```
DES-3200-28F:4# 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-3200-28F:4#
```

config cfm mep

Purpose	This command is used to configure the parameters of a previously created CFM MEP.
Syntax	config cfm mep [mepname <string 32> mepid <int 1-8191> md <string 22> ma <string 22>] {state [enable disable] ccm [enable disable] pdu_priority <int 0-7> fault_alarm [all mac_status remote_ccm error_ccm xcon_ccm none] alarm_time < centisecond 250-1000> alarm_reset_time < centisecond 250-1000> } (1)
Description	<p>An MEP generates five different types of Fault Alarms. The five alarm types are listed with their priorities from high to low as follows:</p> <ul style="list-style-type: none"> 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 <p>If multiple types of the faults occur on an MEP, only the fault with the highest priority will be used for the alarm.</p>
Parameters	<p>mepname <string 32> - The name used for the MEP. The MEP must first be created with the create cfm mep command.</p> <p>mepid <int 1-8191> - This is to specify the MEP identifiers contained in the maintenance association. This must first be created with the config cfm ma command, mepid_list [add delete] <mepid_list> option.</p> <p>ma <string 22> - The name of the previously created maintenance association (MA).</p> <p>md <string 22> - The name of the previously created maintenance domain (MD).</p> <p>state - The administrative state of the MEP.</p> <ul style="list-style-type: none"> enable - MEP is enabled. disable - MEP is disabled. This is the default value. <p>ccm - The CCM transmission state.</p> <ul style="list-style-type: none"> enable - CCM transmission enabled. disable - CCM transmission disabled. This is the default value. <p>pdu_priority - The 802.1p priority is set in the CCMs and the LTMs messages transmitted by the MEP. The default value is 7.</p> <p>fault_alarm - This is the control types of the fault alarms sent by the MEP.</p> <ul style="list-style-type: none"> all - All types of fault alarms will be sent. mac_status - Only the fault alarms whose priority is equal to or higher than "Some Remote MEP MAC Status Errors" are sent. remote_ccm - Only the fault alarms whose priority is equal to or higher than "Some Remote MEPs Down" are sent. error_ccm - Only the fault alarms whose priority is equal to or higher than "Error CCM Received" are sent. xcon_ccm - Only the fault alarms whose priority is equal to or higher than "Cross-connect CCM Received" are sent. none - No fault alarm is sent. This is the default value. <p>alarm_time - This is the time used to control the duration of time the fault alarm is continuously sent when a defect is reported. The unit used is centisecond, the range is 250-1000. The default value is 250.</p> <p>alarm_reset_time - If a fault alarm has not been detected since the previous defect report, this is the time period used to reset. The unit is centisecond, the range is 250-1000. The default value is 1000.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure parameters for MEP “mep1”:

```
DES-3200-28F:4# config cfm mep mep1 state enable ccm enable
Command: config cfm mep mep1 state enable ccm enable

Success.

DES-3200-28F:4#
```

delete cfm mep

Purpose	This command is used to delete a previously created MEP.
Syntax	delete cfm mep [mepname <string 32> mepid <int 1-8191> md <string 22> ma <string 22>]
Description	This command is used to remove a previously created MEP.
Parameters	<p>mepname <string 32> - The name used for the MEP that will be removed.</p> <p>mepid <int 1-8191> - This is to specify the MEP identifiers contained in the maintenance association. This must first be created with the config cfm ma command, mepid_list [add delete] <mepid_list> option.</p> <p>md <string 22> - The name of the previously created maintenance domain (MD).</p> <p>ma <string 22> - The name of the previously created maintenance association (MA).</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To remove a MEP named “mep1”:

```
DES-3200-28F:4# delete cfm mep mep1
Command: delete cfm mep mep1

Success.

DES-3200-28F:4#
```

delete cfm ma

Purpose	This command is used to delete a previously created maintenance association.
Syntax	delete cfm ma <string 22> md <string 22>
Description	All MEPs created in the maintenance association will be deleted automatically.
Parameters	ma <string 22> - The name of the maintenance association (MA) being removed. md <string 22> - The name of the maintenance domain (MD) associated with the deleted MA.
Restrictions	Only Administrator-level users can issue this command.

Example usage :

To remove the MA “op1”:

```
DES-3200-28F:4# delete cfm ma op1 md op_domain
Command: delete cfm ma op1 md op_domain

Success.

DES-3200-28F:4#
```

delete cfm md

Purpose	This command is used to delete a previously created maintenance domain.
Syntax	delete cfm md <string 22>
Description	All the MEPs and maintenance associations created in the maintenance domain will be deleted automatically.
Parameters	md <string 22> - The name of the maintenance domain (MD) being removed.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To remove the MD “op_domain”:

```
DES-3200-28F:4# delete cfm md op_domain
Command: delete cfm md op_domain

Success.

DES-3200-28F:4#
```

enable cfm

Purpose	This command is used to enable the CFM globally.
Syntax	enable cfm
Description	This command is used to enable the CFM globally.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To globally enable CFM on the Switch:

```
DES-3200-28F:4# enable cfm
Command: enable cfm

Success.

DES-3200-28F:4#
```

disable cfm

Purpose	This command is used to disable the CFM globally.
Syntax	disable cfm
Description	This command is used to disable the CFM globally.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable CFM on the Switch:

```
DES-3200-28F:4# disable cfm
Command: disable cfm

Success.

DES-3200-28F:4#
```

config cfm ports

Purpose	This command is used to enable or disable the CFM function on a per-port basis.
Syntax	config cfm ports <portlist> state [enable disable]
Description	By default, the CFM function is disabled on all ports. If the CFM is disabled on a port the following conditions apply: MIPs are never created on that port. MEPs can still be created on that port, and the configuration can be saved. MEPs created on that port can never generate or process CFM PDUs. If the user issues a Loopback or Link trace test on those MEPs, it will prompt the user to inform them that the CFM function is disabled on that port.
Parameters	ports <portlist> - The list of logical ports to be configured. state - [enable disable] - Enables or disables the CFM function on the listed ports.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure CFM state for ports 2-5:

```
DES-3200-28F:4# config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

DES-3200-28F:4#
```

show cfm ports

Purpose	This command is used to show the CFM state of specified ports.
Syntax	show cfm ports <portlist>
Description	This command is used to show the CFM state for specified ports.
Parameters	ports <portlist> - The list of logical ports for which to display CFM configuration.
Restrictions	None.

Example usage

To view CFM settings for ports 3-6:

```
DES-3200-28F:4# show cfm ports 3-6
Command: show cfm ports 3-6

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

DES-3200-28F:4#
```

show cfm	
Purpose	This command is used to show the CFM configuration.
Syntax	show cfm { [md <string 22> { ma <string 22> { mepid <int 1-8191> } } mepname <string 32>] }
Description	This command is used to show the CFM configuration.
Parameters	md <string 22> The name of the maintenance domain (MD) to view CFM settings. ma <string 22> The name of the maintenance association (MA) to view CFM settings. mepid <1-8191> - MEP identifier for CFM settings displayed for MEP. mep <string 32> - MEP name for CFM settings displayed for MEP.
Restrictions	None.

Example usage:

To view CFM settings:

```
DES-3200-28F:4# show cfm
Command: show cfm

CFM State: enabled

Level  MD Name
-----  -
2      op_domain

DES-3200-28F:4#
```

To view CFM settings for MD “op_domain” MA “op1”:

```
DES-3200-28F:4# show cfm md op_domain ma op1
Command: show cfm md op_domain ma op1

MA VID      : 1
MIP Creation : none
CCM Interval : 10 second(s)
SenderID TLV : Defer
MEPID List  : 1, 3, 6-7, 12-15

MEPID  Direction  Port      Name      MAC Address
-----  -
  1     inward     1        mep1     00-20-a2-00-00-01

MIP Port    MAC Address
-----
  3         00-00-61-00-01-00

DES-3200-28F:4#
```

To view CFM settings for MEP “mep1”:

```
DES-3200-28F:4# show cfm mepname mep1
Command: show cfm mepname mep1

Name           : mep1
MEPID          : 1
Port           : 1
Direction      : inward
CFM Port State : enabled
MAC Address    : 00-04-a8-00-00-03
MEP State      : enabled
CCM State      : enabled
PDU Priority   : 7
Fault Alarm    : mac_status
Alarm Time     : 2 second(s)
Alarm Reset Time : 10 second(s)
Highest Fault  : Some Remote MEP Down
Out-of-Sequence CCMs: 0 received
Cross-connect CCMs : 0 received
Error CCMs     : 0 received
Port Status CCMs : 0 received
If Status CCMs : 0 received
CCMs transmitted : 1234
In-order LBRs  : 0 received
Out-of-order LBRs : 0 received
Next LTM Trans ID : 27
Unexpected LTRs : 0 received
LBMs Transmitted : 0

Remote
MEPID  MAC Address      Status  RDI  PortSt  IfSt      Detect Time
-----
2      00-00-61-00-01-00  OK      Yes  Blocked Up        2008-01-01 12:00:00
3      00-00-03-00-01-01  OK      No   Up       Up        2008-01-01 12:00:00
4      00-00-62-00-01-22  OK      No   Up       Down     2008-01-01 12:00:00
8      00-00-61-00-01-00  START   No   Up       Up        2008-01-01 12:00:00
12     00-00-00-00-01-00  FAILED  No   Up       Up        2008-01-01 12:00:00
8      00-00-a8-00-00-00  OK      No   Up       Up        2008-01-01 12:00:00

DES-3200-28F:4#
```

Abbreviations used in the **show cfm** command interface are as follows:

- **Port Status CCMs** - Port Status Defect CCMs.
- **If Status CCMs** - Interface Status Defect CCMs.
- **PortSt** - Port Status TLV in the last received CCM.
- **IfSt** - Interface Status TLV in the last received CCM.

show cfm fault

Purpose	This command is used to show the MEPs that have faults.
Syntax	show cfm fault { md <string 22> { ma <string 22> } }

show cfm fault

Description	This command displays 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.
Parameters	ma <string 22> - The name of the maintenance association (MA) to view faults for MEPs. md <string 22> - The name of the maintenance domain (MD) to view faults for MEPs.
Restrictions	None.

Example usage

To view all MEP faults:

```
DES-3200-28F:4# show cfm fault
Command: show cfm fault

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

DES-3200-28F:4#
```

show cfm port

Purpose	This command is used to show MEPs and MIPs created on a port.
Syntax	show cfm port <port> {level <int 0-7> direction [inward outward] vlanid <vlanid 1-4094>}
Description	This command is used to show the MEPs and MIPs created on a port.
Parameters	port <portlist> - The port for which to display CFM configuration. level <int 0-7> - Setting level of the MD to be shown. If not specified, all levels are shown. direction - The direction of the MEP to be displayed. inward - Inward facing (up) MEP only are displayed. outward - Outward facing (down) MEP only are displayed. If not specified, both directions and the MIP are shown. vlanid <vlanid 1-4094> - VLAN identifier for settings displayed. If not specified, all VLANs are shown.
Restrictions	None.

Example usage:

To display CFM configuration for port 1:

```
DES-3200-28F:4# show cfm port1
Command: show cfm port1

MAC Address: 00-05-78-82-32-01

MD Name      MA Name      MEPID Level Direction VID
-----
op_domain    opl          1      2      inward  2
cust_domain  cust1        8      4      inward  2
serv_domain  serv2        MIP    3              2

DES-3200-28F:4#
```

cfm loopback

Purpose	This command is used to start a CFM loopback test.
Syntax	cfm loopback <macaddr> [mepname <string 32> mepid <int 1-8191> md <string 22> ma <string 22>] {num <int 1-65535> [length <int 0-1500> pattern <string 1500>] pdu_priority <int 0-7> }
Description	<p>Press Ctrl+C to exit the loopback test.</p> <p>The MAC address represents the destination MEP or MIP that can be reached by this MAC address.</p> <p>The MEP represents the source MEP from which to initiate the loopback message.</p>
Parameters	<p><macaddr> - The destination MAC address targeted for testing.</p> <p>mepname <string 32> - The MEP name of the MEP where the test is initiated.</p> <p>mepid <int 1-8191> - The MEP identifier of the MEP where the test is initiated.</p> <p>ma <string 22> - The name of the maintenance association (MA) where the test is initiated.</p> <p>md <string 22> - The name of the maintenance domain (MD) where the test is initiated.</p> <p>num <int 1-65535> - Number of LBMs to be sent. The default value is 4.</p> <p>length <int 0-1500> - The payload length of the LBM to be sent. The default is 0.</p> <p>pattern <string 1500> - An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included.</p> <p>pdu_priority <int 0-7> - 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.</p>
Restrictions	None.

Example usage

To initiate a loopback test from MEP “mep1”:

```
DES-3200-28F:4# cfm loopback 00-01-02-03-04-05 mep mep1
Command: cfm loopback 00-01-02-03-04-05 mep mep1

Request timed out.
Request timed out.
Reply from MPID 52: bytes=xxx time=xxxms
Request timed out.

CFM loopback statistics for 00-01-02-03-04-05:
  Packets: Sent=4, Received=1, Lost=3(75% loss).

DES-3200-28F:4#
```

cfm linktrace

Purpose	This command is used to issue a CFM link trace message.
Syntax	cfm linktrace <macaddr> [mepname <string 32> mepid <int 1-8191> md <string 22> ma <string 22>] {ttl <int 2-255> pdu_priority <int 0-7>}
Description	This command is used to issue a CFM link trace message.
Parameters	<p><macaddr> - The destination MAC address targeted for trace.</p> <p>mepname <string 32> - The MEP name of the MEP where the trace is initiated.</p> <p>mepid <int 1-8191> - The MEP identifier of the MEP where the trace is initiated.</p> <p>md <string 22> - The name of the maintenance domain (MD) where the trace is initiated.</p> <p>ma <string 22> - The name of the maintenance association (MA) where the trace is initiated.</p> <p>ttl <int 2-255> - Link trace message TTL value. The default value is 64.</p> <p>pdu_priority <int 0-7> - The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MEP.</p>
Restrictions	None.

Example usage:

To initiate an link trace from MEP “mep1”:

```
DES-3200-28F:4# cfm linktrace 00-01-02-03-04-05 mep mep1
Command: cfm linktrace 00-01-02-03-04-05 mep mep1

Transaction ID: 26
Success.

DES-3200-28F:4#
```

show cfm linktrace

Purpose	This command is used to show the link trace responses.
Syntax	show cfm linktrace [mepname <string 32> mepid <int 1-8191> md <string 22> ma <string 22>] { trans_id <uint>}
Description	This command is used to display the link trace responses to a CFM link trace. The maximum link trace responses a device can hold is 128.
Parameters	mepname <string 32> - The MEP name of the MEP where the trace is initiated. mepid <int 1-8191> - The MEP identifier of the MEP where the trace is initiated. md <string 22> - The name of the maintenance domain (MD) where the trace is initiated. ma <string 22> - The name of the maintenance association (MA) where the trace is initiated. trans_id <uint> - Identifier of the transaction to show.
Restrictions	None.

Example usage

To view link trace results for trace of MEP “mep1”:

```
DES-3200-28F:4# show cfm linktrace mep mep1
Command: show cfm linktrace mep mep1

Trans ID  Source MEP      Destination
-----  -
26        mep1             00-20-a2-00-00-01

DES-3200-28F:4#
```

To view link trace results for trace of MEP “mep1” transaction “tras_id 26”:

```
DES-3200-28F:4# show cfm linktrace mep mep1 trans_id 26
Command: show cfm linktrace mep mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 00-20-a2-00-00-01
Start Time 2008-01-01 12:00:00

Hop  MEPID  MAC Address          Forwarded  Relay Action
-----
  1      00-00-30-00-20-00   Yes       FDB
  2      00-00-00-00-50-00   Yes       MPDB
  3      00-00-b8-05-00-00   No        Hit

DES-3200-28F:4#
```


delete cfm linktrace

Purpose	This command is used to delete received link trace responses.
Syntax	delete cfm linktrace { [md <string 22> { ma <string 22> { mepid <int 1-8191> } } mepname <string 32>] }
Description	This command is used to delete the stored link trace response data that have been initiated by the specified MEP.
Parameters	md <string 22> - The name of the maintenance domain (MD) where the trace responses are deleted. ma <string 22> - The name of the maintenance association (MA) where the trace responses are deleted. mepname <string 32> - The MEP name of the MEP where the trace responses are deleted. mepid <int 1-8191> - The MEP identifier of the MEP where the trace responses are deleted.
Restrictions	None.

Example usage:

To remove link trace responses from MEP “mep1”:

```
DES-3200-28F:4# delete cfm linktrace mepname mep1
Command: delete cfm linktrace mepname mep1

Success.

DES-3200-28F:4#
```

show cfm mipccm

Purpose	This command is used to display the MIP CCM database entries.
Syntax	show cfm mipccm
Description	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.
Parameters	None.
Restrictions	None.

Example usage

To view the MIP CFM data base:

```
DES-3200-28F:4# show cfm mipccm
Command: show cfm mipccm

MA          VID  MAC Address          Port
-----
opma        1    00-00-b8-05-00-00   2
opma        1    00-00-01-03-00-04   3

Total: 2

DES-3200-28F:4#
```

config cfm mp_ltr_all

Purpose	This command is used to enable or disable the "all MPs reply LTRs" function.
Syntax	config cfm mp_ltr_all [enable disable]
Description	This function is only for test purposes. According to IEEE 802.1ag, a Bridge replies with one LTR to an LTM. This command can make all MPs on the LTM's forwarding path reply with LTRs, no matter whether or not they are on a bridge.
Parameters	enable - Enables the feature. disable - Disables this feature.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable all MPs to reply to LTM:

```
DES-3200-28F:4# config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

DES-3200-28F:4#
```

show cfm mp_ltr_all

Purpose	This command is used to show the current configuration of the "all MPs reply LTRs" function.
Syntax	show cfm mp_ltr_all
Description	This command is used to show the current configuration of the "all MPs reply LTRs" function.
Parameters	None.
Restrictions	None.

Example usage

To view MP reply LTR function status:

```
DES-3200-28F:4# show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Enabled

DES-3200-28F:4#
```

show cfm remote_mep

Purpose	This command is used to display remote MEPs.
Syntax	show cfm remote_mep [md <string 22> ma <string 22> mepid <int 1-8191> mepname <string 32>] remote_mepid <int 1-8191>
Description	This command displays remote MEP information.
Parameters	<p>ma <string 22> - The name of the maintenance association (MA) of the remote MEP to view.</p> <p>md <string 22> - The name of the maintenance domain (MD) of the remote MEP to view.</p> <p>mepid <int 1-8191> - The MEP identifier of the local MEP</p> <p>mepname <string 32> The name of the local MEP.</p> <p>remote_mepid <int 1-8191> - The name of the remote MEP</p>
Restrictions	None.

Example usage:

To view remote MEP information for remote MEP ID "2":

```
DES-3200-28F:4# 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-3200-28F:4#
```

show cfm pkt_cnt

Purpose	This command is used to show the CFM packet's RX/TX counters.
Syntax	show cfm pkt_cnt { [ports <portlist> { [rx tx] } [rx tx] ccm] }
Description	CFM packet counters will be shown.
Parameters	ports <portlist> - Specifies the port counters to show. If not specified, all ports will be shown. {[rx tx]} - Show RX or TX counter. If not specified, both of them will be shown. [rx tx] - Show RX or TX counter. Ccm - CCM RX counters.
Restrictions	None.

Example usage

To display the CFM packet counters on ports 1-12:

```
DES-3200-28:4#show cfm pkt_cnt ports 1-12
Command: show cfm pkt_cnt ports 1-12

CFM RX Statistics
-----
Port    AllPkt    CCM      LBR      LBM      LTR      LTM
-----
all     696       696      0        0        0        0
1       0         0        0        0        0        0
2       696       696      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
```

```

-----
Port  VidDrop  OpcoDrop
-----
all   0         0
1     0         0
2     0         0
3     0         0
4     0         0
5     0         0
6     0         0
7     0         0
8     0         0
9     0         0
10    0         0
11    0         0
12    0         0

CFM TX Statistics
-----
Port  AllPkt  CCM      LBR      LBM      LTR      LTM
-----
all   6358    6358    0        0        0        4
1     0       0       0        0        0        0
2     578    578    0        0        0        4
3     578    578    0        0        0        0
4     578    578    0        0        0        0
5     578    578    0        0        0        0
6     578    578    0        0        0        0
7     578    578    0        0        0        0
8     578    578    0        0        0        0
9     578    578    0        0        0        0
10    578    578    0        0        0        0
11    578    578    0        0        0        0
12    578    578    0        0        0        0

DES-3200-28:4#

```

Example usage:

To display the CFM packet CCM counters:

```
DES-3200-28:4# 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
mep1	1	1	2	inward	9	8	100
mep2	1	2	2	inward	9	8	100
mep3	1	3	2	inward	9	8	100
Total:					27	24	300

clear cfm pkt_cnt

Purpose	This command is used to clear the CFM packet's RX/TX counters.
Syntax	clear cfm pkt_cnt { [ports <portlist> { [rx tx] } [rx tx] ccm] }
Description	CFM packet counters will be cleared.
Parameters	ports <portlist> - The ports which require need the counters clearing. If not specified, all ports will be cleared. {[rx tx]} - Clear RX or TX counters. If none is specified, both of them are cleared. [rx tx] - Clear only RX or TX counters. ccm - Clear only CCM RX counters.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear all CFM packet counters:

```
DES-3200-28F:4# clear cfm pkt_cnt
Command: clear cfm pkt_cnt

Success.

DES-3200-28F:4#
```


ETHERNET OAM COMMANDS

Ethernet OAM (Operations, Administration, and Maintenance) is a data link layer protocol which provides network administrators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions on point-to-point and emulated point-to-point Ethernet link. Ethernet OAM commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config ethernet_oam ports (mode)	[<portlist> all] mode [active passive]
config ethernet_oam ports (state)	[<portlist> all] state [enable disable]
config ethernet_oam ports (link monitor error symbol)	[<portlist> all] link_monitor error_symbol { threshold <number> window < milliseconds 1000-60000> notify_state [enable disable] } (1)
config ethernet_oam ports (link monitor error frame)	[<portlist> all] link_monitor error_frame { threshold <number> window < milliseconds 1000-60000> notify_state [enable disable] } (1)
config ethernet_oam ports (link monitor error frame seconds)	[<portlist> all] link_monitor error_frame_seconds { threshold <number> window < milliseconds 10000-900000> notify_state [enable disable] } (1)
config ethernet_oam ports (link monitor error frame period)	[<portlist> all] link_monitor error_frame_period { threshold <number> window <number 14881- 89286000 > notify_state [enable disable] } (1)
config ethernet_oam ports (critical link event)	[<portlist> all] critical_link_event { dying_gasp critical_event } notify_state [enable disable]
config ethernet_oam ports (remote loopback)	[<portlist> all] remote_loopback [start stop]
config ethernet_oam ports (received remote loopback)	[<portlist> all] received_remote_loopback [process ignore]
show ethernet_oam ports (status)	{<portlist>} status
show ethernet_oam ports (configuration)	{<portlist>} configuration
show ethernet_oam ports (statistics)	{<portlist>} statistics
show ethernet_oam ports (event log)	{ <portlist>} event_log { index <value_list>}
clear ethernet_oam ports (statistics)	[<portlist> all] statistics
clear ethernet_oam ports (event log)	{<portlist> all } event_log

Each command is listed, in detail, in the following sections:

config ethernet_oam ports (mode)

Purpose	Used to configure Ethernet OAM mode for ports.
Syntax	config ethernet_oam ports [<portlist> all] mode [active passive]
Description	<p>The command is used to configure Ethernet OAM for ports to operate in active or passive mode.</p> <p>Port configured in active mode:</p> <ol style="list-style-type: none"> (1) Initiate the exchange of Information OAMPDUs as defined by the discovery state diagram. (2) Active port is permitted to send any OAMPDU while connected to a remote OAM peer entity in active mode. (3) Active port operates in a limited respect if the remote OAM entity is operating in passive mode. (4) Active port should not respond to OAM remote loopback commands and variable requests from a passive peer. <p>Port configured in passive mode:</p> <ol style="list-style-type: none"> (1) Do not initiate the discovery process (2) React to the initiation of the Discovery process by the remote. This eliminates the possibility of passive-to-passive links. (3) Shall not send Variable request or loopback Control OAMPDUs” for describe the active and passive mode.
	 <p>Note: When a port is OAM-enabled, changing the OAM mode will cause the OAM discovery to be re-started</p>
Parameters	<p><portlist> - Specifies a range of ports to be configured. Use all to specify all ports.</p> <p>mode - Specify to operate in either active mode or passive mode. The default mode is active.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure port 1 OAM mode to passive:

```
DES-3200-28F:4# config ethernet_oam ports 1 mode passive
Commands: config ethernet_oam ports 1 mode passive

Success

DES-3200-28F:4#
```


config ethernet_oam ports (state)

Purpose	Used to enable or disable Ethernet OAM per port.
Syntax	config ethernet_oam ports [<portlist> all] state [enable disable]
Description	<p>The command is used to enable or disable Ethernet OAM function on a per port basis.</p> <p>Enabling OAM initiates OAM discovery on a port. When OAM is enabled on a port in active mode, that port will initiate discovery; if the port is not OAM enabled, the port will not participate in the discovery process.</p> <p>If the OAM status of an enabled port changes to disabled, the port sends a dying gasp notice to a peer(s) before disconnecting the OAM link.</p>
Parameters	<p><portlist> - Specifies a range of ports to be configured. Use all to specify all ports.</p> <p>state - Specify to enable or disable the OAM function for the listed ports. The default state is disabled.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable Ethernet OAM on port 1:

```
DES-3200-28F:4# config ethernet_oam ports 1 state enable
Commands: config ethernet_oam ports 1 state enable

Success

DES-3200-28F:4#
```

config ethernet_oam ports (link monitor error symbol)

Purpose	Used to configure Ethernet OAM link monitoring symbol error configuration for ports.
Syntax	config ethernet_oam ports [<portlist> all] link_monitor error_symbol { threshold <number> window < milliseconds 1000-60000> notify_state [enable disable] } (1)
Description	<p>The command is used to configure Ethernet OAM link monitoring symbol error for ports.</p> <p>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.</p>
Parameters	<p><portlist> - Specifies a range of ports to be configured. Use all to specify all ports.</p> <p>threshold - Specify the number of symbol errors in the period that must be equal to or greater than in order for the event to be generated. The default value of the threshold is 1 symbol error.</p> <p>window - The range is 1000 to 60000 ms. The default value is 1000ms.</p> <p>notify_state - Specify to enable or disable event notification. The default state is enable.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DES-3200-28F:4# config ethernet_oam ports 1 link_monitor error_symbol threshold 2 window 1000
notify_state enable
Commands: config ethernet_oam ports 1 link_monitor error_symbol threshold 2 window 1000
notify_state enable

Success

DES-3200-28F:4#
```

config ethernet_oam ports (*link monitor error frame*)

Purpose	Used to configure Ethernet OAM link monitoring error frame configuration for ports.
Syntax	config ethernet_oam ports [<portlist> all] link_monitor error_frame { threshold <number> window < milliseconds 1000-60000> notify_state [enable disable] } (1)
Description	The command used to configure Ethernet OAM link monitoring error frames for ports. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counts of 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.
Parameters	<portlist> - Specifies a range of ports to be configured. Use all to specify all ports. threshold - Specify the number of frame errors in the period that must be equal to or greater than in order for the event to be generated. The default value is 1 frame error. window - The range is 1000 to 60000 ms. The default value is 1000ms. notify_state - Specify to enable or disable event notification. The default state is enable.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DES-3200-28F:4# config ethernet_oam ports 1 link_monitor error_frame threshold 2 window 1000
notify_state enable
Commands: config ethernet_oam ports 1 link_monitor error_frame threshold 2 window 1000
notify_state enable

Success

DES-3200-28F:4#
```

config ethernet_oam ports (*link monitor error frame seconds*)

Purpose	Used to configure Ethernet OAM link monitoring error frame seconds configuration for ports.
Syntax	config ethernet_oam ports [<portlist> all] link_monitor error_frame_seconds

config ethernet_oam ports (link monitor error frame seconds)

	{ threshold <number> window < milliseconds 10000-900000> notify_state [enable disable] } (1)
Description	The command used to configure Ethernet OAM link monitoring error frame seconds for ports. An error frame second is one second interval wherein at least one frame error was detected. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counts of the number of frame errors as well as the number of coding symbol errors. When the number of error frame seconds is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame seconds summary event to notify the remote OAM peer.
Parameters	<portlist> - Specifies a range of ports to be configured. Use all to specify all ports. threshold - Specify the number of error frame seconds in the period must be equal to or greater than in order for the event to be generated. The default value of threshold is 1 error frame second. window - Specify the period of error frame seconds summary event. The range is 10000ms-900000ms and the default value is 60000 ms. notify_state - Specify to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DES-3200-28F:4# config ethernet_oam ports 1 link_monitor error_frame_seconds threshold 2
window 10000 notify_state enable
Commands: config ethernet_oam ports 1 link_monitor error_frame_seconds threshold 2 window
10000 notify_state enable

Success

DES-3200-28F:4#
```

config ethernet_oam ports (link monitor error frame period)

Purpose	Used to configure Ethernet OAM link monitoring error frame period for ports.
Syntax	config ethernet_oam ports [<portlist> all] link_monitor error_frame_period { threshold <number> window <number 14881- 89286000 > notify_state [enable disable] } (1)
Description	The command used to configure ports Ethernet OAM link monitoring error frame period. 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 error frames is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame period event to notify the remote OAM peer.
Parameters	<portlist> - Specifies a range of ports to be configured. Use all to specify all ports. threshold - Specify the number of error frames in the period that must be equal to or greater than in order for the event to be generated. The default value of threshold is 1 error frame. window - Specify the period of error frame period event. The period is specified by a number of received frames. The following rules apply: The default value is the number of 64-byte frames that can be received in one second on the underlying physical layer. The lower bound is the number of 64-byte frames that can be received in 100 ms on the underlying physical layer. The upper bound is the number of 64-byte frames that can be received in one minute on the underlying physical layer. The range for this setting is 14881 to 89286000. The default value for FE ports is 148810 and for GE ports it is 1488100. notify_state - Specify to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the error frame threshold to 10 and period to 100000 for port 1:

```
DES-3200-28F:4# config ethernet_oam ports 1 link_monitor error_frame_period threshold 10 window
100000 notify_state enable
Commands: config ethernet_oam ports 1 link_monitor error_frame_period threshold 10 window
100000 notify_state enable

Success
DES-3200-28F:4#
```

config ethernet_oam ports (*critical link event*)

Purpose	Used to configure Ethernet OAM critical link event for ports.												
Syntax	config ethernet_oam ports [<portlist> all] critical_link_event { dying_gasp critical_event } notify_state [enable disable]												
Description	<p>The command used to configure the capability of Ethernet OAM critical link event. If the capability for an event is disabled, the port will not send out the corresponding critical link event.</p> <p>This table lists conditions that generate a critical link event:</p> <table border="1"> <thead> <tr> <th>Condition</th> <th>Event</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>System reboot</td> <td>Dying gasp</td> <td>If a reboot command is input (CLI, WEB or MIB), the dying gasp event will be sent out first, and then restart the device.</td> </tr> <tr> <td>OAM disable</td> <td>Critical event</td> <td>If the OAM state changes from enable to disable for management, a critical event shall be sent out.</td> </tr> <tr> <td>Port shutdown</td> <td>Critical event</td> <td>If the administrator shuts down the port, critical event will be sent out first before shutdown of the port.</td> </tr> </tbody> </table>	Condition	Event	Description	System reboot	Dying gasp	If a reboot command is input (CLI, WEB or MIB), the dying gasp event will be sent out first, and then restart the device.	OAM disable	Critical event	If the OAM state changes from enable to disable for management, a critical event shall be sent out.	Port shutdown	Critical event	If the administrator shuts down the port, critical event will be sent out first before shutdown of the port.
Condition	Event	Description											
System reboot	Dying gasp	If a reboot command is input (CLI, WEB or MIB), the dying gasp event will be sent out first, and then restart the device.											
OAM disable	Critical event	If the OAM state changes from enable to disable for management, a critical event shall be sent out.											
Port shutdown	Critical event	If the administrator shuts down the port, critical event will be sent out first before shutdown of the port.											
Parameters	<p><portlist> - Specifies a range of ports to be configured. Use all to specify all ports.</p> <p>dying_gasp - An unrecoverable local failure condition has occurred</p> <p>critical_event - An unspecified critical event has occurred.</p> <p>notify_state - Specify to enable or disable the event notification. The default state is enable.</p>												
Restrictions	Only Administrator-level users can issue this command.												

Example usage :

To enable dying gasp notification event for port 1:

```
DES-3200-28F:4# config ethernet_oam ports 1 critical_link_event dying_gasp notify_state enable
Commands: config ethernet_oam ports 1 critical_link_event dying_gasp notify_state enable
```

Success

```
DES-3200-28F:4#
```

config ethernet_oam ports (remote loopback)

Purpose	Used to start or stop Ethernet OAM remote loopback mode for the remote peer of the port.
Syntax	config ethernet_oam ports [<portlist> all] remote_loopback [start stop]
Description	<p>The command is used to start or stop the remote peer to enter Ethernet OAM remote loopback mode.</p> <p>To start the remote peer to enter remote loopback mode, the port must be in active mode and the OAM connection established.</p> <p>If the local client is already in remote loopback mode, then the command cannot be applied.</p>
Parameters	<p><portlist> - Specifies a range of ports to be configured. Use all to specify all ports.</p> <p>remote_loopback - If start is specified, a request is sent to the remote peer to change to remote loopback mode. If stop is specified, a request is sent to the remote peer to change to normal operation mode.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To start remote loopback on port 1 of unit 1:

```
DES-3200-28F:4# config ethernet_oam ports 1 remote_loopback start
Commands: config ethernet_oam ports 1 remote_loopback start

Success

DES-3200-28F:4#
```

config ethernet_oam ports (received remote loopback)

Purpose	Used to configure the method to process the received Ethernet OAM remote loopback command.
Syntax	config ethernet_oam ports [<portlist> all] received_remote_loopback [process ignore]
Description	<p>The command is used to configure the client to process or to ignore a received Ethernet OAM remote loopback command.</p> <p>In remote loopback mode, user traffic is not forwarded on the port. If ignore is specified for received_remote_loopback, the specified port will ignore all requests to transition to remote loopback mode and prevent the Switch from entering remote loopback mode, thus it continues to process user traffic regardless.</p>
Parameters	<p><portlist> - Specifies a range of ports to be configured. Use all to specify all ports.</p> <p>received_remote_loopback - Specify whether to process or ignore the received Ethernet OAM remote loopback command.</p> <p>ignore – The port disregards requests to change to remote loopback mode and continues to forward user traffic.</p> <p>process – The port will accept and process requests to change to remote loopback mode, meaning that it will discontinue forwarding user traffic if it receives a remote loopback mode request.</p> <p>The default method is “ignore”.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DES-3200-28F:4# config ethernet_oam ports 1 received_remote_loopback
process
Commands: config ethernet_oam ports 1 received_remote_loopback process

Success

DES-3200-28F:4#
```

show ethernet_oam ports (status)

Purpose	Used to display primary controls and status information for Ethernet OAM per port.
Syntax	show ethernet_oam ports {<portlist>} status
Description	<p>The command used to show primary controls and status information for Ethernet OAM on specified ports.</p> <p>The information includes:</p> <ol style="list-style-type: none"> (1) OAM administration status: enabled or disabled (2) OAM operation status. It maybe the below value: <ul style="list-style-type: none"> • 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.

show ethernet_oam ports (status)

- **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 Functions Supported:** The OAM functions supported on this port. These functions include:
- **Unidirectional:** It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).
 - **Loopback:** It indicates that the OAM entity can initiate and respond to loopback commands.
 - **Link Monitoring:** It indicates that the OAM entity can send and receive Event Notification OAMPDUs.
 - **Variable:** It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB
- (7) **Loopback Status:** The current status of the loopback function of the port:
- **No Loopback** – The local and remote ports are not in loopback mode.
 - **Initiating Loopback** – The local port has sent the start remote loopback request to the peer and is waiting for response.
 - **Remote Loopback** – This indicates that both the local and remote ports entered the loopback mode. Any non-OAM packet received in the local port will be dropped.
 - **Local Loopback** – This indicates that both the local and remote ports entered the loopback mode. The local port is doing the loopback. Any non-OAM packets received on the port will be sent back to the same port.
 - **Terminate Loopback** - The port is stopping loopback on the port.

Parameters <portlist> - Specifies a range of ports to display status.

Restrictions None.

Example usage

To show OAM control and status information on port 1-2:

```
DES-3200-28F:4# show ethernet_oam ports 1-2 status
Commands: show ethernet_oam ports 1-2 status

Port 1
-----
Local Client OAM      : Disabled
Mode                  : Active
Max OAMPDU            : 1518 Bytes
Remote Loopback       : Support
Unidirectional        : Not Supported
Link Monitoring       : Support
Variable Request      : Not Supported
PDU Revision          : 1
Operation Status      : Operational
Loopback Status       : No Loopback

Port 2
-----
Local Client OAM      : Enabled
Mode                  : Active
Max OAMPDU            : 1518 Bytes
Remote Loopback       : Support
Unidirectional        : Not Supported
Link Monitoring       : Support
Variable Request      : Not Supported
PDU Revision          : 1
Operation Status      : Operational
Loopback Status       : No Loopback

Remote Client
Mode                  : Passive
MAC Address           : 00-01-02-03-04-05
Vendor (OUI)          : 01-80-C2
Max OAMPDU            : 1518 Bytes
Unidirectional        : Supported
Link Monitoring       : Supported
Variable Request      : Supported
PDU Revision          : 1

DES-3200-28F:4#
```

show ethernet_oam ports (configuration)

Purpose	Used to display Ethernet OAM configuration per port.
Syntax	show ethernet_oam ports {<portlist>} configuration
Description	Use this to view Ethernet OAM configurations for ports.
Parameters	<portlist> - Specifies a range of ports to display configurations.
Restrictions	None.

Example usage:

To show Ethernet OAM configuration on port 1-2:

```

DES-3200-28F:4# show ethernet_oam ports 1-2 configuration
Commands: show ethernet_oam ports 1-2 configuration
Port 1
-----
OAM                               : Enabled
Mode                               : Active
Dying GASP                         : Enabled
Critical Event                     : Enabled
Remote Loopback OAMPDU            : Processed
Symbol Error
  Notify State                     : Enabled
  Window:                          : 1000 milliseconds
  Threshold:                       : 1 Error Symbol
Frame Error
  Notify State                     : Enabled
  Window:                          : 1000 milliseconds
  Threshold:                       : 1 Error Frame
Frame Period Error
  Notify State                     : Enabled
  Window:                          : 148810 Frames
  Threshold:                       : 1 Error Frame
Frame Seconds Error
  Notify State                     : Enabled
  Window:                          : 60000 milliseconds
  Threshold:                       : 1 Error Frame

Port 2
-----
OAM                               : Disabled
Mode                               : Active
Dying GASP                         : Enabled
Critical Event                     : Enabled
Remote Loopback OAMPDU            : Processed
Symbol Error
  Notify State                     : Enabled
  Window:                          : 1000 milliseconds
  Threshold:                       : 1 Error Symbol
Frame Error
  Notify State                     : Enabled
  Window:                          : 1000 milliseconds
  Threshold:                       : 1 Error Frame
Frame Period Error
  Notify State                     : Enabled
  Window:                          : 148810 Frames
  Threshold:                       : 1 Error Frame
Frame Seconds Error
  Notify State                     : Enabled
  Window:                          : 10000 milliseconds
  Threshold:                       : 1 Error Frame
DES-3200-28F:4#
    
```

show ethernet_oam ports (statistics)

Purpose	Used to display Ethernet OAM statistics for ports.
Syntax	show ethernet_oam ports {<portlist>} statistics
Description	Use this command to display Ethernet OAM ports statistics information.
Parameters	<portlist> - Specifies a range of ports to display configurations. Use all to specify all ports.
Restrictions	None.

Example usage

To show port 1 OAM statistics:

```
DES-3200-28F:4# show ethernet_oam ports 1 statistics
Commands: 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 Rx OAMPDU : 0
Duplicate Event Notification OAMPDU Tx : 0
Duplicate Event Notification OAMPDU Rx : 0
Loopback Control OAMPDU Tx      : 0
Loopback Control OAMPDU Rx      : 0
Variable Request OAMPDU Tx      : 0
Variable Request OAMPDU Rx      : 0
Variable Response OAMPDU Tx     : 0
Variable Response OAMPDU Rx     : 0
Organization Specific OAMPDU Tx : 0
Organization Specific OAMPDU Rx : 0
Unsupported OAMPDU Tx           : 0
Unsupported OAMPDU Rx           : 0
Frames Lost Due To OAMU         : 0
DES-3200-28F:4#
```

show ethernet_oam ports (event log)

Purpose	Used to display Ethernet OAM event log
Syntax	show ethernet_oam { <portlist> } event_log { index <value_list> }
Description	Use this command to view ports Ethernet OAM event log information. The Switch can buffer 1000 event logs. The event log is different from sys-log. It provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog. Specify an index to show a range of events.
Parameters	<portlist> - Specifies a range of ports to display event logs. Use all to specify all ports. index - Specifies an index range to display.
Restrictions	None.

Example usage:

To show port 1 OAM event:

```
DES-3200-28F:4# show ethernet_oam ports 1 event_log
Commands: show ethernet_oam ports 1 event_log

Port 1
-----
Event Listing
Index   Type                               Location      Time Stamp
-----
1       Error Symbol                        Local         2008-4-18 10:30
        Value: 3, window: 30000ms, threshold: 3, Accumulated errors: 10
2       Error Frame Seconds Remote         2008-4-18 10:35
        Value: 5,window: 1000, threshold: 3, Accumulated errors: 10
3       Dying Gasp                          Remote        2008-4-18 10:35

Local Event Statistics
Error Symbol Event           : 1
Error Frame Event            : 1
Error Frame Period Event     : 0
Errored Frame Seconds Event  : 0
Dying Gasp                   : 0
Critical Event               : 0

Remote Event Statistics
Error Symbol Event           : 1
Error Frame Event            : 1
Error Frame Period Event     : 0
Errored Frame Seconds Event  : 0
Dying Gasp                   : 1
Critical Event               : 0

DES-3200-28F:4#
```

clear ethernet_oam ports (statistics)

Purpose	Used to clear Ethernet OAM port statistics.
Syntax	clear ethernet_oam ports [<portlist> all] statistics
Description	Use this command to clear Ethernet OAM ports statistics information.

clear ethernet_oam ports (*statistics*)

Parameters <portlist> - Specifies a range of ports to clear OAM statistics. Use all to specify all ports.

Restrictions Only Administrator-level users can issue this command.

Example usage

To clear port 1 OAM statistics:

```
DES-3200-28F:4# clear ethernet_oam ports 1 statistics
Commands: clear ethernet_oam ports 1 statistics

Success

DES-3200-28F:4#
```

clear ethernet_oam ports (*event log*)

Purpose Used to clear Ethernet OAM event log for ports.

Syntax clear ethernet_oam ports {<portlist> | all } event_log

Description Use this command to clear ports Ethernet OAM event log information.

Parameters <portlist> - Specifies a range of ports to clear the OAM event log. Use all to specify all ports.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To clear port 1 OAM event log:

```
DES-3200-28F:4# clear ethernet_oam ports 1 event_log
Commands: clear ethernet_oam ports 1 event_log

Success

DES-3200-28F:4#
```

BPDU ATTACK PROTECTION COMMANDS

The BPDU Attack Protection commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
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> } }

Each command is listed, in detail, in the following sections:



Note: The BPDU Attack Protection function and Spanning Tree Protocol for ports are mutually exclusive. When the STP function is enabled on a particular port, BPDU Attack Protection cannot be enabled. If BPDU Attack Protection function is enabled on a port, BPDU cannot be forwarded.

config bpdu_protection ports

Purpose	Used to configure the BPDU Attack Protection state and mode of a port.
Syntax	config bpdu_protection ports[<portlist> all] {state [enable disable] mode [drop block shutdown] } (1)
Description	<p>This command is used to setup the BPDU Attack Protection function for the ports on the switch.</p> <p>The config bpdu_protection ports command is used to configure the BPDU protection function for ports on the Switch. There are two states of BPDU attack protection function; the normal state and the under attack state. The under attack state has three modes: drop, block, and shutdown modes. A BPDU attack protection enabled port will enter under attack state when it receives an STP BPDU frame, then take action based on the configuration mode. BPDU attack protection can ONLY be used for ports that do not have STP enabled.</p> <p>STP for ports and BPDU attack protection on ports are not compatible. Furthermore BPDU attack protection enabled on a port effectively disables all STP function on the port. Keep in mind the following points regarding this:</p> <p>BPDU attack protection has a higher priority than STP BPDU forwarding (i.e. the fbpdu setting of the config stp command is enabled) when determining how to handle BPDU. That is, when fbpdu is enabled to forward STP BPDU frames AND the BPDU attack protection function is enabled, the port will not forward STP BPDU frames.</p> <p>BPDU attack protection has a higher priority than BPDU tunnel port setting (i.e. config bpdu_tunnel ports command) when determining how to handle BPDU. That is, when BPDU tunneling is enabled on a port AND the BPDU attack protection function is enabled, then BPDU tunneling is effectively disabled on the port.</p>
Parameters	<p>portlist – Specifies a range of ports to be configured.</p> <p>all – In order to set all ports in the system, you may use the “all” parameter.</p> <p>state – Specifies the state of BPDU Attack Protection. The default state is disable.</p> <p>enable – Enables the port or ports for BPDU Attack Protection.</p> <p>disable – Disables the port or ports for BPDU Attack Protection.</p> <p>mode – Specifies the BPDU Attack Protection mode.</p> <p>drop – Will drop all RX BPDU packets when the port enters under attack state.</p> <p>block – Will drop all RX packets (include BPDU and normal packets) when the port enters under attack state.</p> <p>shutdown – Will shut down the port when the port enters the under attack state.</p>



Note: The RX BPDU Attack Protection takes effect only when the port enters under attack state while in drop and block mode.

Restrictions	Only Administrator-level users can issue this command.
---------------------	--

Example usage:

To set the BPDU attack protection port state to enable and drop mode:

```
DES-3200-28F:4# config bpdu_protection ports 1 state enable mode drop
Commands: config bpdu_protection ports 1 state enable mode drop

Success.

DES-3200-28F:4#
```

config bpdu_protection recovery_timer

Purpose	Used to configure the BPDU Attack Protection recovery timer.
Syntax	config bpdu_protection recovery_timer [<sec 60-1000000> infinite]
Description	When a port enters under attack state, it can be disabled or blocked based on the configuration. The state can be recovered manually or by the auto recovery mechanism. This command is used to configure the auto-recovery timer. To manually recover the port, the user needs to disable and re-enable the port.
Parameters	<p>recover_timer – Specifies the recovery timer. The default value of recovery timer is 60.</p> <p><sec 60-1000000> – The timer (in seconds) used by the auto-recovery mechanism to recover the port. The valid range is 60 to 1000000.</p> <p>infinite – The port will not be auto recovered.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the BPDU Attack Protection recovery timer to 120 second for the entire switch:

```
DES-3200-28F:4# config bpdu_protection recovery_timer 120
Commands: config bpdu_protection recovery_timer 120

Success.

DES-3200-28F:4#
```

config bpdu_protection trap/log

Purpose	Used to configure trap and log settings for BPDU attack protection events.
Syntax	config bpdu_protection [trap log] [none attack_detected attack_cleared both]
Description	Use this command to configure the trap and log state for BPDU attack protection and specify the type of event sent or logged.
Parameters	<p>none – Specifies that events will not be logged or trapped for both cases.</p> <p>trap – Specifies the trap state. The default state is both trap and log.</p> <p>log – Specifies the log state. The default state is both trap and log.</p> <p>attack_detected – Specifies that events will be logged or trapped when a BPDU attack is detected.</p> <p>attack_cleared – Specifies that events will be logged or trapped when the BPDU attack is cleared.</p> <p>both – Specifies that events will be logged or trapped for both cases.</p> <p>The default setting for log is both and for trap is none.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the trap state for BPDU attack protection events to send traps for attacks detected and attacks cleared:

```
DES-3200-28F:4# config bpdu_protection trap both
Commands: config bpdu_protection trap both

Success.

DES-3200-28F:4#
```

enable bpdu_protection

Purpose Used to globally enable BPDU attack protection on the Switch.

Syntax enable bpdu_protection

Description Use this to enable BPDU attack protection.



NOTE: The BPDU Attack Protection function and Spanning Tree Protocol for ports are mutually exclusive. When the STP function is enabled on a particular port, BPDU Attack Protection cannot be enabled.

Parameters None.

Restrictions Only Administrator-level users can issue this command.

Example usage

To enable BPDU attack protection on the entire Switch:

```
DES-3200-28F:4# enable bpdu_protection
Commands: enable bpdu_protection

Success.

DES-3200-28F:4#
```

disable bpdu_protection

Purpose	Used to disable BPDU attack protection on the Switch.
Syntax	disable bpdu_protection
Description	Use this to disable BPDU attack protection on the entire Switch. Note that if BPDU attack protection is disabled globally, it will also be disabled for ports regardless of the config bpdu_protection ports settings.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable BPDU attack protection on the entire Switch:

```
DES-3200-28F:4# disable bpdu_protection
Commands: disable bpdu_protection

Success.

DES-3200-28F:4#
```

show bpdu_protection

Purpose	Used to display BPDU attack protection settings on the Switch.
Syntax	show bpdu_protection {ports {<portlist> }}
Description	Use this to view the global or per port BPDU attack protection configuration.
Parameters	ports – Specify to view the BPDU attack protection port configuration. <portlist>- Specify the ports to display. If none is specified, all ports BPDU attack protection configuration will be listed.
Restrictions	None.

Example usage:

To display global settings for BPDU protection:

```
DES-3200-28F:4# 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-3200-28F:4#
```

Example usage:

To display BPDU protection settings for ports:

```
DES-3200-28F:4# 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-3200-28F:4#
```

PER-QUEUE BANDWIDTH CONTROL COMMANDS

The Per-Queue Bandwidth Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config per_queue bandwidth_control	{ ports [<portlist> all] } <cos_id_list> { max_rate [no_limit <value 64-1024000 >] } (1)
show per_queue bandwidth_control	{<portlist>}

Each command is listed, in detail, in the following sections:

config per_queue bandwidth_control

Purpose	Used to configure bandwidth control applied to a specific hardware priority queue on a per port basis.
Syntax	config per_queue bandwidth_control { ports [<portlist> all] } <cos_id_list> { max_rate [no_limit <value 64-1024000 >] } (1)
Description	The config per queue bandwidth_control command is used to set egress bandwidth control for a specific priority queue on specified ports. The bandwidth limit is defined by the max_rate value which can be specified with a value between 64Kbps and 1024000Kbps (1 gigabit). When a limit is set with max_rate, frames transmitted from the queue will not exceed the specified limit even when bandwidth is available. The effective bandwidth limit is independent of what mode is used to clear the queue, that is, the limit is in effect at the specified rate if the queue is operating in strict mode or weighted round robin mode.
Parameters	<p>ports - <portlist> – Specifies a range of ports to be configured for bandwidth control.</p> <p>all – Specifies that the bandwidth control be applied to all ports in the system. If the ports parameter is not specified, the system will apply to all ports.</p> <p>cos_id_list - Specifies a list of priority queues. The priority queue number is ranged from 0 to 3.</p> <p>max_rate - Specifies that one of the parameters below (no_limit or <value 64-1024000>) will be applied to the maximum rate at which the above specified class will be allowed to transmit packets.</p> <p>no_limit – Specifies that there will be no limit on the rate of packets received or sent by the above specified class.</p> <p><value 64-1024000> – Specifies the bandwidth ceiling in Kbps for the max_rate.</p> <p>If the specified rate is not multiple of minimum granularity, the rate will be adjusted: Actual rate = rate entered/ minimum granularity * minimal granularity, for example: 62.5= 100/62.5 *62.5 100/62.5 equals the closest smaller integer</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the ports 1-10 per queue bandwidth queue 1 max rate to 100000:

```
DES-3200-28F:4# config per_queue bandwidth_control ports 1-10 1 max_rate
100000
Command: config per_queue bandwidth_control ports 1-10 1 max_rate 100000

Success.

DES-3200-28F:4#
```

show per_queue bandwidth_control

Purpose	Used to display the configuration settings for per-queue bandwidth control.
Syntax	show per_queue bandwidth_control {<portlist>}
Description	Use this command to view the per-queue bandwidth limits set for each port.
Parameters	<portlist> – Specifies a range of ports for which to display the current bandwidth control configuration.
Restrictions	None.

Example usage

To view the bandwidth control configuration for port number 10:

```
DES-3200-28F:4# show per_queue bandwidth_control 10
Command: show per_queue bandwidth_control 10

Queue Bandwidth Control Table On Port: 10

Queue           Max_Rate (Kbit/sec)
-----
0                62500
1                no_limit
2                no_limit
3                no_limit

DES-3200-28F:4#
```


ERPS COMMANDS

The Ethernet Ring Protection Switching (ERPS) defined in ITU-T G.8032 is intended to provide a protection switching and recovery process, and to prevent loops forming for Ethernet in a ring topology. The ERPS commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
enable erps	
disable erps	
create erps raps_vlan	<vlanid>
delete erps raps_vlan	<vlanid>
config erps raps_vlan	<vlanid> ring_mel <value 0-7>
config erps raps_vlan	<vlanid> ring_port [west <port> east <port>]
config erps raps_vlan	<vlanid> [rpl_port [west east none] rpl_owner [enable disable]]
config erps raps_vlan	<vlanid> protected_vlan [add delete] vlanid <vidlist>
config erps raps_vlan	<vlanid> timer { holdoff_time <millisecond 0-10000> guard_time <millisecond 10-2000 > wtr_time <min 5-12>} (1)
config erps log	[enable disable]
show erps	
config erps trap	[enable disable]

Each command is listed, in detail, in the following sections:

enable erps

Purpose	Used to enable the global ERPS function on the Switch.
Syntax	enable erps
Description	This command is used to enable the global ERPS function on the Switch. For each ring with the ring state enabled when ERPS is enabled, the following integrity will be checked: <ol style="list-style-type: none"> 1. A 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. The default state is ERPS disabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To globally enable ERPS:

```
DES-3200-28F:4# enable erps
Command: enable erps

Success.

DES-3200-28F:4#
```

disable erps

Purpose	Used to disable ERPS function on the Switch. The default setting on the Switch is ERPS disabled.
Syntax	disable erps
Description	This will disable ERPS on the Switch. The default setting is ERPS disabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To globally disable ERPS:

```
DES-3200-28F:4# disable erps
Command: disable erps

Success.

DES-3200-28F:4#
```

create erps VLAN

Purpose	Used to define an existing VLAN as an R-APS VLAN on the Switch.
Syntax	create erps raps_vlan <vlanid>
Description	Use this command to create a special R-APS VLAN that is used for transferring R-APS control messages. Note: The R-APS VLAN must already have been created with the create vlan command.
Parameters	raps_vlan <vlanid> - Designates the VLAN identified by the vlanid as the R-APS VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an R-APS VLAN:

```
DES-3200-28F:4# create erps raps_vlan 4094
Command: create erps raps_vlan 4094

Success.

DES-3200-28F:4#
```

delete erps VLAN

Purpose	Used to remove an R-APS VLAN on the Switch.
Syntax	delete erps raps_vlan <vlanid>
Description	This command will remove the R-APS VLAN as well all its configured parameters. This command can only be issued when the ring is not active.
Parameters	raps_vlan <vlanid> - Designates the VLAN identified by the vlanid as the R-APS VLAN to be removed.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To remove an R-APS VLAN and its associated parameters:

```
DES-3200-28F:4# delete erps raps_vlan 4094
Command: delete erps raps_vlan 4094

Success.

DES-3200-28F:4#
```

config erps ring_mel

Purpose	Used to configure the MEL (maintenance entity group level) value.
Syntax	config erps raps_vlan <vlanid> ring_mel <value 0-7>
Description	<p>This command is used to configure the ring MEL for an R-APS VLAN. The ring MEL is one field in the R-APS PDU.</p> <p>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 (maintenance entity group end point) with the same VLAN on the ring ports, the R-APS PDU cannot be forwarded on the ring.</p>
Parameters	<p>raps_vlan <vlanid> - Designates the VLAN identified by the vlanid as the R-APS VLAN to be configured for a MEL value.</p> <p>ring_mel <value 0-7> - Specifies the ring MEL value. The default value is 1.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the ring MEL for R-APS VLAN 4094:

```
DES-3200-28F:4# config erps raps_vlan 4094 ring mel 2
Command: config erps raps_vlan 4094 ring mel 2

Success.

DES-3200-28F:4#
```

config erps ring_port

Purpose	Used to configure the ports of the ERPS ring for a specific R-APS VLAN.
Syntax	config erps raps_vlan <vlanid> ring_port [west <port> east <port>]
Description	<p>This command is used to configure the port that participates in the ERPS ring. Restrictions apply for ports that are included in a link aggregation group. A link aggregation group can be configured as a ring port by specifying the master port of the link aggregation port. Only the master port can be specified as a ring port. If the specified link aggregation group is eliminated, the master port retains its ring port status.</p> <p>Note: Ring ports cannot be modified when ERPS is enabled.</p>
Parameters	<p>raps_vlan <vlanid> - Designates the VLAN identified by the vlanid as the R-APS VLAN where ring ports are being defined.</p> <p>Each node in a ring topology has two ports related to the ring, one in each direction that connects to the next node so that the first node ultimately connects to the last node forming the ring. The direction of these connections are distinguished using the cardinal direction labels “east” and “west”.</p> <p>west <port> : Specifies the port as the west ring port.</p> <p>east <port> : Specifies the port as the east ring port.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To designate the west and east ring ports:

```
DES-3200-28F:4# config erps raps_vlan 4094 ring_port west 5 east 7
Command: config erps raps_vlan 4094 ring_port west 5 east 7

Success.

DES-3200-28F:4#
```

config erps rpl

Purpose	Used to define the RPL port or the RPL owner status for a specific R-APS VLAN.
Syntax	config erps raps_vlan <vlanid> [rpl_port [west east none] rpl_owner [enable disable]]
Description	<p>This command is used to configure the RPL port and the RPL owner in an R-APS VLAN. Use rpl_port to define the west or east port as an RPL port. To remove the RPL port status, use rpl_port none to indicate that neither the west or east port are RPL ports.</p> <p>Use rpl_owner to designate the node as the RPL owner. RPL owner status can be enabled or disabled.</p> <p>ERPS must first be globally disabled to modify the RPL owner or RPL port configuration.</p>
Parameters	<p>raps_vlan <vlanid> - Designates the VLAN identified by the vlanid as the R-APS VLAN where the node is being configured.</p> <p>port – Define the west or east port as an RPL port; or remove RPL status from the node by specifying none.</p> <p>Default setting, the node does not have an RPL port.</p> <p>rpl_owner - Used to determine RPL owner status.</p> <p> enable - Designates the device as an RPL owner node.</p> <p> disable - This node is not an RPL owner.</p> <p>By default, the RPS owner is disabled.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To define RPL owner status for the west port of R-APS VLAN 4094:

```
DES-3200-28F:4# config erps raps_vlan 4094 rpl port west owner enable
Command: config erps raps_vlan 4094 rpl port west owner enable

Success.

DES-3200-28F:4#
```

config erps protected VLAN

Purpose	Used to configure the protected VLAN for a specific R-APS VLAN.
Syntax	config erps raps_vlan <vlanid> protected_vlan [add delete] vlanid <vidlist>
Description	This command is used to designate VLANs that are protected by the ERPS function. The R-APS VLAN cannot be a 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.
Parameters	<p>raps_vlan <vlanid> - Designates the VLAN identified by the vlanid as the R-APS VLAN where another VLAN can be defined as being a member of the protected VLAN group.</p> <p>protected_vlan – add or delete protected status for a VLAN specified by the vlanid <vidlist> parameter that follows.</p> <p> add – To add VLAN to protected VLAN group</p> <p> delete – To remove VLAN to protected VLAN group</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure protected VLAN status for VLANs 10-20:

```
DES-3200-28F:4# 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-3200-28F:4#
```

config erps timer

Purpose	Used to configure ERPS timers for an R-APS VLAN.
Syntax	<vlanid> timer { holdoff_time <millisecond 0-10000> guard_time <millisecond 10-2000 > wtr_time <min 5-12>} (1)
Description	<p>This command is used to configure the ERPS protocol timers on a specified R-APS VLAN. The timers are defined as follows:</p> <p>Holdoff timer - 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.</p> <p>Guard timer - 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. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.</p> <p>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.</p>
Parameters	<p>laps_vlan <vlanid> - Designates the VLAN identified by the vlanid as the R-APS VLAN where the timers are applied</p> <p>holdoff_time < millisecond 0-10000> - Specifies the holdoff time of the R-APS function. The default holdoff time is 0 milliseconds.</p> <p>guard_time < millisecond 10-2000> - Specifies the guard time of the R-APS function. The default guard time is 500 milliseconds.</p> <p>wtr_time <min 5-12> - Specifies the WTR time of the R-APS function. The range is from 5 to 12 minutes. The default WTR time is 5 minutes.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure ERPS timers on R-APS VLAN 4094:

```
DES-3200-28F:4# config erps laps_vlan 4094 holdoff_time 100 guard_time 1000 wtr_time 10
Command: config erps laps_vlan 4094 holdoff_time 100 guard_time 1000 wtr_time 10

Success.

DES-3200-28F:4#
```

config erps log

Purpose	Used to configure the status of the ERPS log function.
----------------	--

config erps log

Syntax	config erps log [enable disable]
Description	This command is used to enable or disable logging of ERPS events.
Parameters	enable disable – Use to define the status of ERPS logging. Logging is disabled by default.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the ERPS logging function:

```
DES-3200-28F:4# config erps log enable
Command: config erps log enable

Success.

DES-3200-28F:4#
```

show erps

Purpose	Used to display ERPS information.
Syntax	show erps
Description	<p>This command is used to display ERPS configuration and operation information.</p> <p>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.</p> <p>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.</p>
Parameters	None.
Restrictions	None.

Example usage:

To display current ERPS information:

```
DES-3200-28F:4# show erps
Command: show erps

ERPS Information
-----
ERPS Status           : Enabled
R-APS VLAN            : 8
West Port             : 25 (Blocking)
East Port             : 26 (Forwarding)
RPL Port             : West Port
Owner                 : Enabled (Active)
Protection VLANs     : 2
Ring MEL              : 1
Holdoff Time         : 0 ms
Guard Time           : 500 ms
WTR Time             : 5 minutes
Log                   : Disabled
Trap                  : Disabled
Current Ring State   : Protection

DES-3200-28F:4#
```

config erps trap	
Purpose	Used to configure the trap status for ERPS.
Syntax	config erps trap [enable disable]
Description	This command is used to enable or disable the trap state for ERPS events.
Parameters	enable disable – Use to define the status of ERPS traps. ERPS traps are disabled by default.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable ERPS traps:

```
DES-3200-28F:4# config erps trap enable
Command: config erps trap enable
Success.

DES-3200-28F:4#
```

NETWORK LOAD BALANCING (NLB) COMMANDS

The Network Load Balancing (NLB) commands are used to configure the Switch to support Network Load Balancing Service, a proprietary Microsoft implementation of server clustering and load balancing, suitable for various stateless applications such as FTP, VPN and Web servers. Client requests for such applications can be distributed among multiple servers in a cluster that share a single IP address and a single destination MAC address. Client requests are forwarded to all servers in the cluster but only one will actually process the request.

The Switch operates NLB in unicast mode or multicast mode. In both modes, a shared destination MAC address is used as the destination MAC address in the client request frame. However, in the server that actually processes the request will use its own MAC address in the reply frame.

Please consult Microsoft's server documentation for more information on using and setting up NLB on Windows servers.

The NLB commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
create nlb unicast_fdb	<macaddr>
delete nlb unicast_fdb	<macaddr>
config nlb unicast_fdb	<macaddr> [add delete] <portlist>
create nlb multicast_fdb	[<vlan_name 32> vlanid <vlanid 1-4094>] <macaddr>
delete nlb multicast_fdb	[<vlan_name 32> vlanid <vlanid 1-4094>] <macaddr>
config nlb multicast_fdb	[<vlan_name 32> vlanid <vlanid 1-4094>] <macaddr> [add delete] <portlist>
show nlb fdb	

Each command is listed, in detail, in the following sections:

create nlb unicast_fdb

Purpose	Used to create an entry for the NLB unicast FDB.
Syntax	create nlb unicast_fdb <macaddr>
Description	<p>For NLB, the Switch uses a FDB that is separate from and independent of the Layer 2 unicast FDB. Since a MAC address entered into the special NLB FDB can and be learned dynamically and entered into the Layer 2 FDB, it is important to make sure the special NLB entry is not allowed to be learned or entered into the Layer 2 FDB.</p> <p>The unicast NLB FDB is needed in order to match the unicast MAC address and the egress ports. If the destination MAC address matches the configured NLB FDB entry, the frame is forwarded directly to the configured egress ports.</p> <p>Important: Network Load Balancing will not function properly if an entry in the NLB Forwarding Data Base is able to be learned and duplicated in the Layer 2 FDB.</p> <p>For clients, the destination MAC address used in the request frame is the same as the shared MAC address. However the server that handles the request uses its own MAC address as the source MAC, not the shared MAC address in the reply frame.</p>
Parameters	<macaddr> - The MAC address being entered into the NLB Forwarding Data Base.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an NLB unicast FDB entry:

```
DES-3200-28F:4# create nlb unicast_fdb 02-bf-01-01-01-01
Command: create nlb unicast_fdb 02-bf-01-01-01-01
Success.
DES-3200-28F:4#
```

delete nlb unicast_fdb

Purpose	Used to remove a previously created MAC address entry from the NLB unicast FDB.
Syntax	delete nlb unicast_fdb
Description	The delete nlb unicast_fdb command is used to remove an entry from the NLB FDB.
Parameters	<macaddr> - The MAC address being removed from the NLB Forwarding Data Base.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To remove an NLB unicast FDB entry:

```
DES-3200-28F:4# delete nlb unicast_fdb 02-bf-01-01-01-01
Command: delete nlb unicast_fdb 02-bf-01-01-01-01
Success.
DES-3200-28F:4#
```

config nlb unicast_fdb

Purpose	Used to configure the forwarding ports for an existing NLB FDB entry; or used to remove previously configured forwarding ports for an NLB FDB entry.
Syntax	config nlb unicast_fdb <macaddr> [add delete] <portlist>
Description	The config nlb unicast_fdb command is used to specify which egress ports are matched to an NLB unicast FDB entry by adding or removing ports on the configured list of forwarding ports.
Parameters	<p><macaddr> - The MAC address of the previously created NLB unicast FDB entry.</p> <p>add – Specifies that the ports listed be added to the NLB unicast FDB as allowed egress ports.</p> <p>delete - Specifies that the ports listed be removed from the NLB unicast FDB as allowed egress ports.</p> <p><portlist> - The list of forwarding ports being added or removed, to be used for the configured NLB unicast FDB entry.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure an NLB unicast FDB entry:

```
DES-3200-28F:4# 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-3200-28F:4#
```

create nlb multicast_fdb

Purpose	Used to create an entry for the NLB multicast FDB.
Syntax	create nlb multicast_fdb [<vlan_name 32> vlanid <vlanid 1-4094>] <macaddr>
Description	The multicast NLB FDB is needed in order to match the multicast MAC address and the egress ports. If the destination MAC address matches the configured NLB multicast FDB entry, the frame is forwarded directly to the configured egress ports.
Parameters	<p><vlan_name 32> - Specifies the name of the VLAN of the NLB multicast FDB entry being created.</p> <p>vlanid <vlanid 1-4094> - Specifies the VLAN ID of the NLB multicast FDB entry being created.</p> <p><macaddr> - The MAC address being entered into the NLB Forwarding Data Base.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To create an NLB multicast FDB entry:

```
DES-3200-28F:4# 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-3200-28F:4#
```

delete nlb multicast_fdb

Purpose	Used to remove a previously created MAC address entry from the NLB multicast FDB.
Syntax	delete nlb multicast_fdb [<vlan_name 32> vlanid <vlanid 1-4094>] <macaddr>
Description	The delete nlb multicast_fdb command is used to delete the NLB multicast FDB entry.
Parameters	<p><vlan_name 32> - Specifies the name of the VLAN of the NLB multicast FDB entry being removed.</p> <p>vlanid <vlanid 1-4094> - Specifies the VLAN ID of the NLB multicast FDB entry being removed.</p> <p><macaddr> - The MAC address being removed from the NLB multicast Forwarding Data Base.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To remove an NLB multicast FDB entry:

```
DES-3200-28F:4# 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-3200-28F:4#
```

config nlb multicast_fdb

Purpose	Used to configure the forwarding ports for an existing NLB multicast FDB entry; or used to remove previously configured forwarding ports for an NLB multicast FDB entry.
Syntax	config nlb multicast_fdb [<vlan_name 32> vlanid <vlanid 1-4094>] <macaddr> [add delete] <portlist>
Description	The config nlb multicast_fdb command is used to specify the VLAN and egress ports that are matched to an NLB multicast FDB entry on the configured list of forwarding ports.
Parameters	<p><vlan_name 32> - Specifies the name of the VLAN of the NLB multicast FDB entry being configured.</p> <p>vlanid <vlanid 1-4094> - Specifies the VLAN ID of the NLB multicast FDB entry being configured.</p> <p><macaddr> - The MAC address of the previously created NLB multicast FDB entry.</p> <p>add - Specifies that the ports listed be added to the NLB multicast FDB as allowed egress ports.</p> <p>delete - Specifies that the ports listed be removed from the NLB multicast FDB as allowed egress ports.</p> <p><portlist> - The list of forwarding ports being added or removed, to be used for the configured NLB multicast FDB entry.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a NLB multicast MAC forwarding database entry:

```
DES-3200-28F:4# 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-3200-28F:4#
```

show nlb fdb

Purpose	Used to display all configured NLB FDB entries.
Syntax	show nlb fdb
Description	This command will display all NLB FDB entries that have been configured.
Parameters	None.
Restrictions	None.

Example usage:

To display the NLB forwarding table for all NLB FDB entries:

```
DES-3200-28F:4# show nlb fdb
Command: show nlb fdb

MAC Address          VLAN ID      Egress Ports
-----
02-bf-01-01-01-01   -            1-5, 26, 26
02-bf-01-01-01-02   -            1-5, 26, 26
03-bf-01-01-01-01   100         1-5, 26, 26
03-bf-01-01-01-01   1           1-5, 26, 26

Total Entries : 4
DES-3200-28F :4#
```


PPPoE CIRCUIT ID INSERTION COMMANDS

PPPoE Circuit ID Insertion is used to produce the unique subscriber mapping capability that is possible on ATM networks between ATM-DSL local loop and the PPPoE server. The PPPoE server will use the inserted Circuit Identifier sub-tag of the received packet to provide AAA services (Authentication, Authorization and Accounting). Through this method, Ethernet networks can be as the alternative of the ATM networks.

The PPPoE Circuit ID Insertion commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameters
config pppoe circuit_id_insertion	state [enable disable]
config pppoe circuit_id_insertion ports	<portlist> { circuit_id [mac ip udf <string 32>] state [enable disable] } (1)
show pppoe circuit_id_insertion	
show pppoe circuit_id_insertion ports	{<portlist>}

Each command is listed, in detail, in the following sections:

config pppoe circuit_id_insertion state

Purpose	Used to enable or disable the PPPoE circuit identifier insertion.
Syntax	config pppoe circuit_id_insertion state [enable disable]
Description	<p>When PPPoE circuit identifier insertion is 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.</p> <p>The inserted circuit ID contains the following information:</p> <ul style="list-style-type: none">Client MAC addressDevice IDPort number <p>By default, the Switch IP address is used as the device ID to encode the circuit ID option.</p>
Parameters	<p>enable – Enables PPPoE circuit ID insertion globally.</p> <p>disable – Disables PPPoE circuit ID insertion.</p> <p>The function is disabled by default.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To globally enable PPPoE circuit identifier insertion:

```
DES-3200-28F:4# config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable

Success.

DES-3200-28F:4#
```

config pppoe circuit_id_insertion ports

Purpose	Used to enable and disable PPPoE circuit identifier insertion on a per port basis and specify how to encode the circuit ID option.
Syntax	config pppoe circuit_id_insertion ports <portlist> { circuit_id [mac ip udf <string 32>] state [enable disable] } (1)
Description	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, inserted by the system, from the received PPPoE offer and session confirmation packet.
Parameters	<p><portlist> - Specifies a list of ports to be configured.</p> <p>state – Specify to enable or disable PPPoE circuit ID insertion for the ports listed. The default settings are enabled for ID insertion per port, but disabled globally.</p> <p>circuit_id - Configures the device ID used for encoding of the circuit ID option.</p> <p>mac – Specifies that the Switch MAC address be used to encode the circuit ID option.</p> <p>ip – Specifies that the Switch IP address be used to encode the circuit ID option.</p> <p>udf – A user defined string to be used to encode the circuit ID option. The maximum length is 32.</p> <p>The default encoding for the device ID option is the Switch IP address.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable port 5 PPPoE circuit ID insertion function and use Host MAC::Switch IP::Host Port as circuit ID value:

```
DES-3200-28F:4# config pppoe circuit_id_insertion ports 5 state enable circuit_id ip
Command: config pppoe circuit_id_insertion ports 5 state enable circuit_id ip

Success.

DES-3200-28F:4#
```

show pppoe circuit_id_insertion

Purpose	Used to display the PPPoE circuit identifier insertion status for the Switch.
Syntax	show pppoe circuit_id_insertion
Description	This will display the global state configuration of the PPPoE circuit ID insertion function.
Parameters	None.
Restrictions	None.

Example usage:

To view the global PPPoE ID insertion state:

```
DES-3200-28F:4# show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Status: Disabled

DES-3200-28F:4#
```

show pppoe circuit_id_insertion ports

Purpose	Used to display the PPPoE ID insertion configuration on a per port basis.
Syntax	show pppoe circuit_id_insertion ports {<portlist>}
Description	This command allows the user to view the configuration of PPPoE ID insertion for each port.
Parameters	<portlist> - Specifies which ports to display. If no ports are specified, all ports configuration will be listed.
Restrictions	None.

Example usage

To view PPPoE circuit ID configuration for ports 2 to 5:

```
DES-3200-28F:4# show pppoe circuit_id_insertion ports 2-5
Command: show pppoe circuit_id_insertion ports 2-5

Port   State          Circucit ID
----   -
2      Disabled      Switch MAC
3      Enabled       UDF String (D_Link-DES30xypD-Link_DES-XXXX)
4      Disabled      Switch IP
5      Enabled       Switch MAC

DES-3200-28F:4#
```

DHCP SERVER SCREENING SETTINGS

Due to this function allow you not only to restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more than one DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

When DHCP Server Screening function is enabled, all DHCP Server packets will be filtered from a specific port. Also, you are allowed to create entries for specific Server IP address and Client MAC address binding by port-based. Be aware that the DHCP Server Screening function must be enabled first. Once all setting is done, all DHCP Server packets will be filtered from a specific port except those that meet the Server IP Address and Client MAC Address binding.

Command	Parameters
config filter dhcp_server	[add permit server_ip <ipaddr> { client_mac <macaddr> } ports [<portlist> all] delete permit server_ip <ipaddr> { client_mac <macaddr> } ports [<portlist> all] ports [<portlist> all] state [enable disable]]
show filter dhcp_server	
config filter dhcp_server trap_log	[enable disable]
config filter dhcp_server illegal_server_log_suppress_duration	[1min 5min 30min]

config filter dhcp_server

Purpose	DHCP server packets except those that have been IP/client MAC bound 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/client binding entry.
Syntax	config filter dhcp_server [add permit server_ip <ipaddr> { client_mac <macaddr>} ports [<portlist> all] delete permit server_ip <ipaddr> { client_mac <macaddr> } ports [<portlist> all] ports [<portlist> all] state [enable disable]]
Description	This command has two purposes: To filter all DHCP server packets on the specified port(s) and to allow some DHCP server packets to be forwarded if they are on the pre-defined server IP address/MAC address binding list. Thus the DHCP server can be restricted to service a specified DHCP client. This is useful when there are two or more DHCP servers present on a network.
Parameters	ipaddr – The IP address of the DHCP server to be filtered macaddr – The MAC address of the DHCP client. state – Enable/Disable the DHCP filter state ports <portlist> – The port number to which the DHCP filter will be applied.
Restrictions	Only Administrator can issue this command.

Example usage:

To add an entry from the DHCP server/client filter list in the switch's database:

```
DES-3200-28F:4#config filter dhcp_server add permit_server_ip 10.1.1.1 client_mac 00-00-00-00-00-01 port all
Command: config filter dhcp_server add permit_server_ip 10.1.1.1 client_mac 00-00-00-00-00-01 port all

Success

DES-3200-28F:4#
```

To configure the DHCP filter state:

```
DES-3200-28F:4#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success

DES-3200-28F:4#
```

show filter dhcp_server

Purpose	Used to display current DHCP server/client filter list created on the switch.
Syntax	show filter dhcp_server
Description	This command is used to display DHCP server/client filter list created on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server filter list created on the switch:

```
DES-3200-28F:4#show filter dhcp_server
Command: show filter dhcp_server

Enabled ports : 1-10
Trap State : Disabled
Log State : Disabled
Illegal_Server_Log_Suppress_Duration : 5 Minutes

Permit DHCP Server/Client Table:
Server IP Address Client MAC address Ports
-----
10.254.254.251      00-1A-92-24-80-F1  1-10

DES-3200-28F:4#
```

config filter dhcp_server trap / log

Purpose	Used to enable or disable the trap and log functions for DHCP server screening.
Syntax	config filter dhcp_server [trap log] [enable disable]
Description	This command will enable or disable traps and logs for DHCP server screening.
Parameters	trap – Specify to enable or disable traps for DHCP server screening. log - Specify to enable or disable logging for DHCP server screening. enable – Enable the log or trap function. disable – Disable the log or trap function.
Restrictions	Only Administrator users can issue this command.

Example usage:

To enable the DHCP server screening trap function.

```
DES-3200-28F:4#config filter dhcp_server trap enable
Command: config filter dhcp_server trap enable

Success.

DES-3200-28F:4#
```

config filter dhcp_server illegal_server_log_suppress_duration

Purpose	Used to configure the suppress duration of illegal DHCP server feature.
Syntax	config filter dhcp_server illegal_server_log_suppress_duration [1min 5min 30min]
Description	Configure the time period to continue to suppress log entries listing illegal DHCP servers for the filter DHCP server screening function. The command is effective immediately and lasts for the period configured.
Parameters	1min – Configure suppress time of 1 minute. 5min – Configure suppress time of 5 minutes. 30min - Configure suppress time of 30 minutes.
Restrictions	Only Administrator users can issue this command.

Example usage:

To configure a suppress duration of illegal DHCP server feature of 5 minutes:

```
DES-3200-28F:4# config filter dhcp_server
illegal_server_log_suppress_duration 5min
Command: config filter dhcp_server illegal_server_log_suppress_duration 5min
Success.

DES-3200-28F:4#
```


APPENDIX A - PASSWORD RECOVERY PROCEDURE

This document 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 document will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.

Power on the switch. After the runtime image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the "Password Recovery Mode". Once the Switch enters the "Password Recovery Mode", all ports on the Switch will be disabled.

```
Boot ProcedureV1.00.006
-----
Power On Self Test ..... 100%

MAC Address   : 00-63-32-28-01-01
H/W Version   : B1

Please wait, loading V1.28.005 Runtime image ..... 100%

The switch is now entering Password Recovery Mode.
```

```
The switch is currently in Password Recovery Mode.
>
```

In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
reset config	The reset config command resets the whole configuration will be back to the default value
reboot	The reboot command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The reset account command deletes all the previously created accounts.
reset password {<username>}	The reset password command resets the password of the specified user. If a username is not specified, the password 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 cold start	System cold start	Critical
	System warm start	System warm start	Critical
	Configuration saved to flash	Configuration saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	Configuration saved to flash by console	Configuration saved to flash by console (Username: <username>)	Informational
	System log saved to flash	System log saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	System log saved to flash by console	System log saved to flash by console (Username: <username>)	Informational
	Configuration and log saved to flash	Configuration and log saved to flash (Username: <username>, IP: <ipaddr>)	Informational
	Configuration and log saved to flash by console	Configuration and log saved to flash by console (Username: <username>)	Informational
Upload/Download	Firmware upgraded successfully	Firmware upgraded successfully (Username: <username>, IP: <ipaddr>)	Informational
	Firmware upgraded by console successfully	Firmware upgraded by console successfully (Username: <username>)	Informational
	Firmware upgrade was unsuccessful	Firmware upgrade was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Firmware upgrade by console was unsuccessful	Firmware upgrade by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully downloaded	Configuration successfully downloaded (Username: <username>, IP: <ipaddr>)	Informational
	Configuration successfully downloaded by console	Configuration successfully downloaded by console (Username: <username>)	Informational
	Configuration download was unsuccessful	Configuration download was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Configuration download by console was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully uploaded	Configuration successfully uploaded (Username: <username>, IP: <ipaddr>)	Informational
	Configuration successfully uploaded by console	Configuration successfully uploaded by console (Username: <username>)	Informational
	Configuration upload was unsuccessful	Configuration upload was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning

	Configuration upload by console was unsuccessful	Configuration upload by console was unsuccessful! (Username: <username>)	Warning
	Log message successfully uploaded	Log message successfully uploaded (Username: <username>, IP: <ipaddr>)	Informational
	Log message successfully uploaded by console	Log message successfully by console uploaded (Username: <username>)	Informational
	Log message upload was unsuccessful	Log message upload was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning
	Log message upload by console was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>)	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
	Login failed through Web (SSL)	Login failed through Web (SSL) due to AAA server timeout or improper configuration	Informational
	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!	Warning
STP	Topology changed	Topology changed (Instance:<InstanceID> port<portNum>)	Informational
	New Root selected	[CIST CIST Regional MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>)	Informational
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational
	Root restriction enabled	Port <portNum> STP root restriction is enabled	Informational
	Root restriction disabled	Port <portNum> STP root restriction is disabled	Informational
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 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 method (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_enable method (Username: <username>)	Informational
Enable Admin failed through SSH authenticated by AAA local_enable method	Enable Admin failed through 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 method (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
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
Successful Enable Admin through Telnet authenticated by AAA	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational

	server		
	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 response is wrong	AAA server <serverIP> (Protocol: <protocolname>) response is wrong	Warning
	AAA doesn't support this functionality.	AAA doesn't support this functionality.	Informational
	AAA server timed out	AAA server <serverIP> (Protocol: <protocol>) connection failed	Warning
Port security	Port security has exceeded its maximum learning size and will not learn any new addresses	Port security violation (Port: <portNum>, MAC: <macaddr>)	Warning
IP-Mac-port Binding	Unauthenticated IP address discarded by IP mac port binding	Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <ipaddr>, MAC <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry is conflict with static ARP	Dynamic IMPB entry is conflicting with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry is conflict with static FDB	Dynamic IMPB entry is conflicting with static FDB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry conflicts with static IMPB	Dynamic IMPB entry is conflicting 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 available(IP:<ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	the number of blocked entries reaches the threshold on a port	Port <portNum> enters stop IMPB learning state.	Warning
	User manually recover from IMPB stop learning state.	Port <portNum> recovers from IMPB stop learning state.	Warning
IP and Password Changed	IP Address change activity	Management IP address was changed into <ipAddr> by (Username: <username>, IP:<ipaddr>)	Informational
	IP Address change activity by console	Management IP address was changed into <ipAddr> by console (Username: <username>)	Informational

	Password change activity	User <username> Password was changed by (Username: <username>, IP:<ipaddr>)	Informational
	Password change activity by console	User <username> Password was changed by console (Username: <username>)	Informational
Safeguard Engine	Safeguard Engine is in normal mode	Safeguard Engine enters NORMAL mode	Informational
	Safeguard Engine is in exhausted mode	Safeguard Engine enters EXHAUSTED mode	Warning
Packet Storm	Broadcast storm occurrence	Port <portNum> Broadcast storm is occurring	Warning
	Broadcast storm cleared	Port <portNum> Broadcast storm has cleared	Informational
	Multicast storm occurrence	Port <portNum> Multicast storm is occurring	Warning
	Multicast storm cleared	Port <portNum> Multicast storm has cleared	Informational
	Port shutdown due to a packet storm	Port <portNum> is currently shutdown due to a packet storm	Warning
Gratuitous ARP	Conflict IP was detected with this device	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>), Interface: <interface>)	Informational
802.1X	Radius server assigned VID: to port	Radius server <server_ip> assigned VID: <VLAN_ID> to Port <portNum> (Account: <user_account>)	Informational
	Radius server assigned ingress bandwidth: Kbits to port	Radius server <server_ip> assigned ingress bandwidth: <bandwidth_value>Kbits to Port<portNum> (Account: <user_account>)	Informational
	Radius server assigned ingress bandwidth: no limit to port	Radius server <server_ip> assigned ingress bandwidth: no limit to Port <portNum> (Account: <user_account>)	Informational
	Radius server assigned egress bandwidth: Kbits to port	Radius server <server_ip> assigned egress bandwidth: <bandwidth_value> Kbits to Port <portNum> (Account: <user_account>)	Informational
	Radius server assigned egress bandwidth: no limit to Port	Radius server <server_ip> assigned egress bandwidth: no limit to Port<portNum> (Account: <user_account>)	Informational
	Radius server assigned 802.1p default priority: to Port	Radius server <server_ip> assigned 802.1p default priority: <priority 0-7> to Port <portNum> (Account: <user_account>)	Informational
	802.1x Authentication failure	802.1x Authentication failure from (Username: <user_account>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication failure for the radius server	802.1x Authentication failure for the radius server <server_ip> timeout from (Username: <user_account>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication failure for the 802.1X client session timeout	802.1x Authentication failure for the 802.1X client session timeout from (Username: <user_account>, Port <portNum>, MAC: <macaddr>)	Warning
	802.1x Authentication success	802.1x Authentication success from (Username: <user_account>, Port <portNum>, MAC: <macaddr>)	Informational
Loopback	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
	VLAN LOOP Max Number exceed	Loop VLAN number overflow	Informational
Denial Service of	The DoS attack is blocked	<dos_name> is detected from (IP: <ipaddr> Port: <portNum>)	Critical
MAC-based Access Control	A host fails to pass the authentication	MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <portNum>, VID: <vid>)	Informational
	A host passes the authentication	MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational
	A host is aged out.	MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational
	Failed to assign ACL profiles/rules from RADIUS server	RADIUS server <ipAddr> assigns <username> ACL failure at port <portNum> (<string>)	Warning
OAM	Dying gasp event(remote)	OAM dying gasp event received (Port <portNum>)	Warning
	Dying gasp event(local)	Device encountered an OAM dying gasp event.	Warning
	Critical event(remote)	OAM critical event event received (Port <portNum>)	Warning
	Critical event(local)	Device encountered an OAM critical event	Warning
	Errored Symbol Period Event(remote)	Errored symbol period event received (Port <portNum>)	Warning
	Errored Frame Event	Errored frame event received(Port <portNum>)	Warning
	Errored Frame Period Event	Errored frame period event received(Port <portNum>)	Warning
	Errored Frame Seconds Summary Event	Errored frame seconds summary event received (Port <portNum>)	Warning
	Remote loopback start	OAM Remote loopback started (Port <portNum>)	Warning
	Remote loopback stop	OAM Remote loopback terminated (Port <portNum>)	Warning
ERPS	Signal fail detected	Signal fail detected on node (MAC: <macaddr>)	Informational
	Signal fail cleared	Signal fail cleared on node (MAC: <macaddr>)	Informational
	RPL owner conflict	RPL owner conflicted on the ring (MAC: <macaddr>)	Warning
BPDU Protection	BPDU attack happened.	Port <portNum> enter BPDU under protection state (mode: drop / block / shutdown)	Informational
	BPDU attack automatically recover	Port <portNum> recover from BPDU under protection state automatically	Informational
	BPDU attack manually recover	Port <portNum> recover from BPDU under protection state manually	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 remote setting error. 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
DHCP Server Screening	Detected untrusted DHCP server IP address.	Detected untrusted DHCP server(IP: <ipaddr>,	Informational

APPENDIX C – TRAP LOG ENTRIES

Trap Name/OID	Variable Bind	Format	MIB Name
coldStart 1.3.6.1.6.3.1.1.5.1	None	V2	RFC1907 (SNMPv2-MIB)
warmStart 1.3.6.1.6.3.1.1.5.2	None	V2	RFC1907 (SNMPv2-MIB)
authenticationFailure 1.3.6.1.6.3.1.1.5.5	None	V2	RFC1907 (SNMPv2-MIB)
linkDown 1.3.6.1.6.3.1.1.5.3	ifIndex, ifAdminStatus, ifOperStatus	V2	RFC2863 (IF-MIB)
linkup 1.3.6.1.6.3.1.1.5.4	ifIndex, ifAdminStatus, ifOperStatus	V2	RFC2863 (IF-MIB)
newRoot 1.3.6.1.2.1.17.0.1	None	V2	RFC1493 (BRIDGE-MIB)
topologyChange 1.3.6.1.2.1.17.0.2	None	V2	RFC1493 (BRIDGE-MIB)
risingAlarm 1.3.6.1.2.1.16.0.1	alarmIndex alarmVariable alarmSampleType alarmValue alarmRisingThreshold	V2	rfc2819 (RMON-MIB)
fallingAlarm 1.3.6.1.2.1.16.0.2	alarmIndex alarmVariable alarmSampleType alarmValue alarmFallingThreshold	V2	rfc2819 (RMON-MIB)
LldpRemTablesChange 1.0.8802.1.1.2.0.0.1	lldpStatsRemTablesInserts lldpStatsRemTablesDeletes lldpStatsRemTablesDrops lldpStatsRemTablesAgeouts	V2	LLDP-MIB
dot1agCfmFaultAlarm	dot1agCfmMepHighestPrDefect	V2	IEEE8021-CFM-MIB
dot3OamThresholdEvent 1.3.6.1.2.1.158.0.1	dot3OamEventLogTimestamp dot3OamEventLogOui dot3OamEventLogType dot3OamEventLogLocation dot3OamEventLogWindowHi dot3OamEventLogWindowLo dot3OamEventLogThresholdHi dot3OamEventLogThresholdLo dot3OamEventLogValue dot3OamEventLogRunningTotal	V2	DOT3-OAM-MIB

	dot3OamEventLogEventTotal		
dot3OamNonThresholdEvent 1.3.6.1.2.1.158.0.2	dot3OamEventLogTimestamp dot3OamEventLogOui dot3OamEventLogType dot3OamEventLogLocation dot3OamEventLogEventTotal	V2	DOT3-OAM-MIB

Proprietary Trap List

Trap Name/OID	Variable Bind	Format	MIB Name
SwIplMacBindingViolationTrap 1.3.6.1.4.1.171.12.23.5.0.1	swIplMacBindingPortIndex swIplMacBindingViolationIP swIplMacBindingViolationMac	V2	IPMacBind-MIB
swIplMacBindingStopLearningTrap 1.3.6.1.4.1.171.12.23.5.0.2	swIplMacBindingPortIndex	V2	IPMacBind-MIB
swIplMacBindingRecoverLearningTrap 1.3.6.1.4.1.171.12.23.5.0.3	swIplMacBindingPortIndex	V2	IPMacBind-MIB
swMacBasedAuthLoggedSuccess 1.3.6.1.4.1.171.12.35.11.1.0.1	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
SwMacBasedAuthLoggedFail 1.3.6.1.4.1.171.12.35.11.1.0.2	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
SwMacBasedAuthAgesOut 1.3.6.1.4.1.171.12.35.11.1.0.3	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
swPktStormOccurred 1.3.6.1.4.1.171.12.25.5.0.1	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB
swPktStormCleared 1.3.6.1.4.1.171.12.25.5.0.2	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB
agentGratuitousARPTrap 1.3.6.1.4.1.171.12.1.7.2.0.5	agentGratuitousARPIpAddr agentGratuitousARPMacAddr agentGratuitousARPPortNumber agentGratuitousARPInterfaceName	V2	Genmgmt-MIB
swSafeGuardChgToExhausted 1.3.6.1.4.1.171.12.19.4.1.0.1	swSafeGuardCurrentStatus	V2	SafeGuard Engine-MIB
swSafeGuardChgToNormal 1.3.6.1.4.1.171.12.19.4.1.0.2	swSafeGuardCurrentStatus	V2	SafeGuard Engine-MIB
swDoSAttackDetected 1.3.6.1.4.1.171.12.59.4.0.1	swDoSCtrlType swDoSNotifyVarIpAddr swDoSNotifyVarPortNumber	V2	DoSPrev-MIB
swSingleIPMSColdStart 1.3.6.1.4.1.171.12.8.6.0.11	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSWarmStart	swSingleIPMSID	V2	SINGLE-IP-MIB

1.3.6.1.4.1.171.12.8.6.0.12	swSingleIPMSMacAddr		
swSingleIPMSLinkDown 1.3.6.1.4.1.171.12.8.6.0.13	swSingleIPMSID swSingleIPMSMacAddr ifIndex	V2	SINGLE-IP-MIB
swSingleIPMSLinkUp 1.3.6.1.4.1.171.12.8.6.0.14	swSingleIPMSID swSingleIPMSMacAddr ifIndex	V2	SINGLE-IP-MIB
swSingleIPMSAuthFail 1.3.6.1.4.1.171.12.8.6.0.15	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSnewRoot 1.3.6.1.4.1.171.12.8.6.0.16	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSTopologyChange 1.3.6.1.4.1.171.12.8.6.0.17	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSrisingAlarm 1.3.6.1.4.1.171.12.8.6.0.18	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSfallingAlarm 1.3.6.1.4.1.171.12.8.6.0.19	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSmacNotification 1.3.6.1.4.1.171.12.8.6.0.20	swSingleIPMSID swSingleIPMSMacAddr swSingleIPMSTrapMessage	V2	SINGLE-IP-MIB
swERPSSFDetectedTrap 1.3.6.1.4.1.171.12.78.4.0.1	swERPSNodeId	V2	ERPS-MIB
swERPSSFClearedTrap 1.3.6.1.4.1.171.12.78.4.0.2	swERPSNodeId	V2	ERPS-MIB
swERPSPLOwnerConflictTrap 1.3.6.1.4.1.171.12.78.4.0.3	swERPSNodeId	V2	ERPS-MIB
swBpduProtectionUnderAttackingTrap 1.3.6.1.4.1.171.12.76.4.0.1	swBpduProtectionPortIndex swBpduProtectionPortMode	V2	BPDU- PROTECTION- MIB
swBpduProtectionRecoveryTrap 1.3.6.1.4.1.171.12.76.4.0.2	swBpduProtectionPortIndex swBpduProtectionRecoveryMethod	V2	BPDU- PROTECTION- MIB
swFilterDetectedTrap 1.3.6.1.4.1.171.12.37.100.0.1	swFilterDetectedIP swFilterDetectedport	V2	FILTER-MIB
swL2PortSecurityViolationTrap 1.3.6.1.4.1.171.11.113.1.1.2.20.0.1 1.3.6.1.4.1.171.11.113.1.2.2.20.0.1 1.3.6.1.4.1.171.11.113.1.3.2.20.0.1 1.3.6.1.4.1.171.11.113.1.4.2.20.0.1	swL2PortSecurityPortIndex swL2PortSecurityViolationMac	V2	des3200-10- L2mgmt.mib des3200-18- L2mgmt.mib des3200-26- L2mgmt.mib des3200-28- L2mgmt.mib des3200-28f- L2mgmt.mib
swL2macNotification 1.3.6.1.4.1.171.11.113.1.1.2.20.0.2 1.3.6.1.4.1.171.11.113.1.2.2.20.0.2 1.3.6.1.4.1.171.11.113.1.3.2.20.0.2	swL2macNotifyInfo	V2	des3200-10- L2mgmt.mib des3200-18- L2mgmt.mib des3200-26-

1.3.6.1.4.1.171.11.113.1.4.2.20.0.2			L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2PortLoopOccurred 1.3.6.1.4.1.171.11.113.1.1.2.20.0.3 1.3.6.1.4.1.171.11.113.1.2.2.20.0.3 1.3.6.1.4.1.171.11.113.1.3.2.20.0.3 1.3.6.1.4.1.171.11.113.1.4.2.20.0.3	swL2LoopDetectPortIndex	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-26-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2PortLoopRestart 1.3.6.1.4.1.171.11.113.1.1.2.20.0.4 1.3.6.1.4.1.171.11.113.1.2.2.20.0.4 1.3.6.1.4.1.171.11.113.1.3.2.20.0.4 1.3.6.1.4.1.171.11.113.1.4.2.20.0.4	swL2LoopDetectPortIndex	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-26-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2VlanLoopOccurred 1.3.6.1.4.1.171.11.113.1.1.2.20.0.5 1.3.6.1.4.1.171.11.113.1.2.2.20.0.5 1.3.6.1.4.1.171.11.113.1.3.2.20.0.5 1.3.6.1.4.1.171.11.113.1.4.2.20.0.5	swL2LoopDetectPortIndex swL2VlanLoopDetectVID	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-26-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2VlanLoopRestart 1.3.6.1.4.1.171.11.113.1.1.2.20.0.6 1.3.6.1.4.1.171.11.113.1.2.2.20.0.6 1.3.6.1.4.1.171.11.113.1.3.2.20.0.6 1.3.6.1.4.1.171.11.113.1.4.2.20.0.6	swL2LoopDetectPortIndex swL2VlanLoopDetectVID	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-26-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.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 priority of the port.	0-7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC-based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign **VLAN by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. To use VLAN assignment, RFC3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	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 ethernet vlan 0xFFF profile_id 100; ACL rule: config access_profile profile_id 100 add access_id auto_assign ethernet vlan_id default port all deny;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: **create access_profile ethernet vlan 0xFFF profile_id 100;** ACL rule: **config access_profile profile_id 100 add access_id auto_assign ethernet;**), and the MAC-based Access Control 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 22 Access Control List (ACL) Commands.