



X S T A C K[®]

CLI MANUAL

PRODUCT MODEL: **xStack[®] DES-3528/DES-3552 SERIES**

LAYER 2 MANAGED STACKABLE FAST ETHERNET SWITCH

RELEASE 2.0

Table of Contents

INTRODUCTION	1
USING THE CONSOLE CLI	3
COMMAND SYNTAX	7
BASIC SWITCH COMMANDS	9
MODIFY BANNER AND PROMPT COMMANDS	22
SWITCH PORT COMMANDS	25
PORT SECURITY COMMANDS	30
STACKING COMMANDS.....	34
NETWORK MANAGEMENT (SNMP) COMMANDS	37
SWITCH UTILITY COMMANDS.....	56
NETWORK MONITORING COMMANDS.....	65
MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS.....	80
FORWARDING DATABASE COMMANDS.....	93
TRAFFIC CONTROL COMMANDS	100
QOS COMMANDS	104
PORT MIRRORING COMMANDS.....	116
VLAN COMMANDS.....	119
VOICE VLAN COMMANDS.....	134
SUBNET-BASED VLAN COMMANDS	141
ASYMMETRIC VLAN COMMANDS.....	144

LINK AGGREGATION COMMANDS	146
IP-MAC-PORT BINDING (IMPB) COMMANDS	151
LIMITED IP MULTICAST ADDRESS	165
BASIC IP COMMANDS	171
MULTICAST VLAN COMMANDS	175
IGMP SNOOPING COMMANDS	192
DHCP RELAY COMMANDS	208
802.1X COMMANDS (INCLUDING GUEST VLANS).....	221
ACCESS CONTROL LIST (ACL) COMMANDS	243
SAFEGUARD ENGINE COMMANDS	264
FILTER COMMANDS (DHCP SERVER/NETBIOS).....	266
L3 CPU FILTER COMMANDS	271
LOOP-BACK DETECTION COMMANDS	273
TRAFFIC SEGMENTATION COMMANDS	277
SFLOW COMMANDS.....	279
TIME AND SNTP COMMANDS.....	288
ARP AND GRATUITOUS ARP COMMANDS	293
ROUTING TABLE COMMANDS	302
MAC NOTIFICATION COMMANDS	304
ACCESS AUTHENTICATION CONTROL COMMANDS	307
SSH COMMANDS	328
SSL COMMANDS	335

D-LINK SINGLE IP MANAGEMENT COMMANDS.....	340
JWAC COMMANDS.....	351
LLDP COMMANDS.....	371
Q-IN-Q COMMANDS.....	385
RSPAN COMMANDS.....	391
STATIC MAC-BASED VLAN COMMANDS.....	395
SIMPLE RED COMMANDS.....	397
MLD SNOOPING COMMAND LIST.....	404
MAC-BASED ACCESS CONTROL COMMANDS LIST.....	419
MULTIPLE AUTHENTICATION COMMANDS.....	430
WEB-BASED ACCESS CONTROL COMMANDS.....	436
POE COMMANDS.....	446
PPPOE CIRCUIT ID INSERTION COMMANDS.....	450
DNS RELAY COMMANDS.....	451
POLICY ROUTE COMMANDS.....	454
BPDU ATTACK PROTECTION COMMANDS.....	457
ETHERNET OAM COMMANDS.....	461
DHCP SERVER COMMANDS.....	472
CABLE DIAGNOSTIC COMMANDS.....	486
CONNECTIVITY FAULT MANAGEMENT COMMANDS.....	488
COMMAND HISTORY LIST.....	505
TECHNICAL SPECIFICATIONS.....	509

MITIGATING ARP SPOOFING ATTACKS VIA PACKET CONTENT ACL	512
PASSWORD RECOVERY PROCEDURE	520

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.

The DES-3528/52 Layer 2 stackable Fast Ethernet Switch Series are members of the D-Link xStack® family. Ranging from 10/100Mbps edge switches to core gigabit switches, the xStack switch family has been future-proof designed to provide a stacking architecture with fault tolerance, flexibility, port density, robust security and maximum throughput with a user-friendly management interface for the networking professional.

This manual provides a reference for all of the commands contained in the CLI for the xStack® DES-3528, DES-3528P, DES-3528DC and DES-3552 series of switches. Configuration and management of the Switch via the Web-based management agent is discussed in the User's Guide.



NOTE: For the remainder of this manual, all versions of the DES-3528, DES-3528P, DES-3528DC and DES-3552 switches will be referred to as simply the Switch or the DES-3528/52 Series.

Accessing the Switch via the Serial Port

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

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

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

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

```
DES-3528 Fast Ethernet Switch
Command Line Interface

Firmware: Build 2.00.B033
Copyright(C) 2009 D-Link Corporation. All rights reserved.
UserName:
```

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-3528:5#**. 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.B007
-----
Power On Self Test ..... 100 %

MAC Address   : 00-21-91-AF-EA-00
H/W Version   : A2

Please wait, loading V2.00.B033 Runtime image ..... 100 %
UART init ..... 100 %
Device Discovery ..... 100 %
Configuration init..... \_
    
```

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 on the Configuration menu.

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

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

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.
2. Alternatively, 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-3528:5#config ipif System ipaddress 10.24.73.21/8
Command: config ipif System ipaddress 10.24.73.21/8

Success.

DES-3528:5#
    
```

Figure 1-3. Assigning an IP Address screen

In the above example, the Switch was assigned an IP address of 10.24.73.21 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 DES-3528/52 Series 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 software 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-232C serial cable. Your terminal parameters will need to be set to:

- **VT-100 compatible**
- **115200 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-3528 Fast Ethernet Switch
Command Line Interface

Firmware: Build 2.00.B033
Copyright(C) 2009 D-Link Corporation. All rights reserved.
UserName:
```

Figure 2-1. Initial Console screen after logging in

Commands are entered at the command prompt, **DES-3528:5#**.

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
cfm linktrace
cfm loopback
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear cfm pkt_cnt
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear ethernet_oam ports
clear fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistic counter
clear jwac auth_state
clear log
clear mac_based_access_control auth_state
clear mld_snooping data_driven_group
clear mld_snooping statistic counter
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 a **Next possible completions:** message.

```

DES-3528:5#config account
Command: config account

Next possible completions:
<username>

DES-3528:5#

```

Figure 2-3. Example Command Parameter Help

In this case, the command **config account** was entered with 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-3528:5#config account
Command: config account
Next possible completions:
<username>

DES-3528:5#config account
Command: config account
Next possible completions:
<username>

DES-3528:5#

```

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-3528:5#the
Available commands:
..                ?                cable_diag        cfm
clear             config           create            debug
delete           disable         download          enable
login            logout          no                ping
reboot           reconfig       reset            save
set              show           telnet           upload

DES-3528:5#
```

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-3528:5#show
Command: show
Next possible completions:
802.1p          802.1x          access_profile  account
accounting      acct_client     address_binding
arp_spoofing_prevention
attack_log      auth_client     arpentry        asymmetric_vlan
auth_session_statistics
authen_enable   authen_login    auth_diagnostics
authen_policy   authentication
authorization    autoconfig     bandwidth_control
cfm             command_history
cpu            cpu_filter      current_config  cos
dhcp           dhcp_local_relay
dnsmr          dot1v_protocol_group
error          ethernet_oam    fdb             filter
firmware       flow_meter      gratuitous_arp  greeting_message
gvrp           hol_prevention igmp_snooping   ipif
iproute        jumbo_frame    jvac            lacp_port
limited_multicast_addr
log            log_save_timing
mac_based_access_control
mac_based_vlan  mac_notification
mcast_filter_profile
mld_snooping   multicast       mef_l2_protocols
mirror
poe            policy_route    port            packet
port_vlan      ports           pppoe           port_security
qinq           radius          router_ports    pvid
safeguard_engine
scheduling     scheduling_mechanism
serial_port     session         sflow           sim
snmp           sntp            sred            ssh
ssl            stack_information
stacking       stp
subnet_vlan    switch          syslog          system_severity
time           time_range     traffic
traffic_segmentation
trusted_host   utilization
vlan           vlan_precedence
vlan_translation
vlan_trunk
voice_vlan     wac
DES-3528:5#

```

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. The online help contained in the CLI and available through the console interface uses the same syntax.



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

<angle brackets>

Purpose	Encloses a variable or value that must be specified.
Syntax	config ipif <ipif_name 12> [{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 <ipif_name 12> 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 Engineering ipaddress 10.24.22.5/255.0.0.0 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 operator 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 Tommy

| vertical bar

Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	create account [admin operator 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 Tommy

{braces}

Purpose	Encloses an optional value or set of optional arguments.
Syntax	reset {[config system]} force_agree
Description	In 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. See the following chapter, Basic Commands for more details about the reset command. 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.
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
create account	[admin operator user] <username 15>
config account	<username> {encrypt [plain_text sha_1] <password>}
show account	
delete account	<username>
enable password encryption	
disable password encryption	
show session	
show switch	
show device_status	
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	
telnet	<ipaddr> {tcp_port <value 0-65535>}
enable telnet	<tcp_port_number 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>
disable web	
save	{[config <config_id 1-2> log all]}
reboot	{force_agree}
reset	{[config system]} {force_agree}
login	
logout	

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

create account

Purpose	Used to create user accounts.
Syntax	create account [admin operator 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 8 user accounts can be created.
Parameters	[admin operator user] <username 15>
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-3528:5#create account admin dlink
Command: create account admin dlink

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

DES-3528:5#
```



NOTICE: In case of lost passwords or password corruption, please refer to the D-Link website and the White Paper entitled “Password Recovery Procedure”, 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	When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password. If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-I.
Parameters	<i><username></i> – Name of the account. The account must already be defined. <i>plain_text</i> – Select to specify the password in plain text form. <i>sha_1</i> – Select to specify the password in the SHA-I encrypted form. <i>password</i> – The password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The assword is case-sensitive.
Restrictions	Only Administrator level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.

Example usage:

To configure the user password of “dlink” account:

```
DES-3528:5#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-3528:5#
```

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 8 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-3528:5#show account
Command: show account

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

Total Entries: 1

DES-3528:5#
```

delete account

Purpose	Used to delete an existing user account.
Syntax	delete account <username>
Description	This command is used to delete an existing entry.
Parameters	<username> – Name of the user who will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account “System”:

```
DES-3528:5#delete account System
Command: delete account System

Success.

DES-3528:5#
```


enable password encryption

Purpose	Used to enable password encryption.
Syntax	enable password encryption
Description	<p>The user account configuration information will be stored in the configuration file, and can be applied to the system later.</p> <p>If the password encryption is enabled, the password will be in encrypted form.</p> <p>When password encryption is disabled, if the user specifies the password in plain text form, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will still be in the encrypted form. It cannot be reverted to the plaintext.</p>
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable password encryption:

```
DES-3528:5#enable password encryption
Command: enable password encryption

Success.

DES-3528:5#
```

disable password encryption

Purpose	Used to disable password encryption.
Syntax	disable password encryption
Description	<p>The user account configuration information will be stored in the configuration file, and can be applied to the system later.</p> <p>If the password encryption is enabled, the password will be in encrypted form.</p> <p>When password encryption is disabled, if the user specifies the password in plain text form, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will still be in the encrypted form. It cannot be reverted to the plaintext.</p>
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable password encryption:

```
DES-3528:5#disable password encryption
Command: disable password encryption

Success.

DES-3528:5#
```

show session

Purpose	Used to display a list of currently logged-in users.
Syntax	show session
Description	This command displays 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-3528:5#show session
Command: show session

ID      Live Time          From              Level   Name
---      -
 8      00:00:16.250      Serial Port       5       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 displays information about the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch's information:

```

DES-3528:5#show switch
Command: show switch

Device Type       : DES-3528 Fast Ethernet Switch
MAC Address       : 00-21-91-53-3E-C8
IP Address        : 10.24.73.21 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.B007
Firmware Version  : Build 2.00.B031
Hardware Version  : A2
Serial Number     : P1UQ28B000010
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
MLD Snooping      : Disabled
VLAN Trunk        : Disabled
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
SNMP              : Disabled
SSL status        : Disabled

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

show device_status

Purpose	Used to display the current Switch power status.
Syntax	show device_status
Description	This command displays status of both the Switch's internal and external power.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch's power status:

```

DES-3528:5#show device_status
Command: show device_status

Internal Power   External Power   Side Fan   Back Fan
-----
      Active           Fail           OK           ---

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

show serial_port

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

Example usage:

To display the serial port setting:

```
DES-3552:5#show serial_port
Command: show serial_port
```

```
Baud Rate      : 115200
Data Bits      : 8
Parity Bits     : None
Stop Bits      : 1
Auto-Logout    : Never
```

```
DES-3552:5#
```

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><i>baud_rate [9600 19200 38400 115200]</i> – The serial bit rate that will be used to communicate with the management host. There are four options: 9600, 19200, 38400, 115200. Factory default setting is 115200.</p> <p><i>never</i> – No time limit on the length of time the console can be open with no user input.</p> <p><i>2_minutes</i> – The console will log out the current user if there is no user input for 2 minutes.</p> <p><i>5_minutes</i> – The console will log out the current user if there is no user input for 5 minutes.</p> <p><i>10_minutes</i> – The console will log out the current user if there is no user input for 10 minutes.</p> <p><i>15_minutes</i> – The console will log out the current user if there is no user input for 15 minutes.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure baud rate:

```
DES-3528:5#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200
```

```
Success.
```

```
DES-3528:5#
```



NOTE: If a user configures the serial port's baud rate, the baud rate will take effect and save immediately. Baud rate settings will not change even if the user resets or reboots the Switch. The Baud rate will only change when the user configures it again. The serial port's baud rate setting is not stored in the Switch's configuration file. Resetting the Switch will not restore the baud rate to the default setting.

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 and Operator-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-3528:5#enable clipaging
Command: enable clipaging

Success.

DES-3528:5#
```

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 and Operator-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-3528:5#disable clipaging
Command: disable clipaging

Success.

DES-3528:5#
```

telnet

Purpose	Used to login the remote device system through the network.
Syntax	telnet <ipaddr> {tcp_port <value 0-65535>}
Description	This command is used when the manager want to manage the device system which isn't on local. So can use this command to login in the remote system which is located on other side. If connect successful, some actions can be done as local.
Parameters	<ipaddr> – The network ip address. This is the destination which wants to login. <value 0-65535> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23.
Restrictions	None.

Example usage:

Telnet to the remote Switch:

```
DES-3528:5#telnet 172.18.168.12 tcp_port 50
Command: telnet 172.18.168.12 tcp_port 50

Connecting to server,please wait....

                DES-3552 Gigabit Ethernet Switch
                Command Line Interface

                Firmware: Build 1.03.B009
                Copyright(C) 2008 D-Link Corporation. All rights reserved.
UserName:
PassWord:
```

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 or UDP 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 and Operator-level users can issue this command.

Example usage:

To enable Telnet and configure port number:

```
DES-3528:5#enable telnet 23
Command: enable telnet 23

Success.

DES-3528:5#
```

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 and Operator-level users can issue this command.

Example usage:

To disable the Telnet protocol on the Switch:

```
DES-3528:5#disable telnet
Command: disable telnet

Success.

DES-3528:5#
```

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	<i><tcp_port_number 1-65535></i> – 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 and Operator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DES-3528:5#enable web 80
Command: enable web 80

Success.

DES-3528:5#
```

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 and Operator-level users can issue this command.

Example usage:

To disable HTTP:

```
DES-3528:5#disable web
Command: disable web

Success.

DES-3528:5#
```

save

Purpose	Used to save changes in the Switch's configuration to non-volatile RAM.
Syntax	save {[config < config_id 1-2> 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	<i>config</i> < <i>config_id</i> 1-2> – Specify to save current settings to configuration file 1 or 2. <i>log</i> – Specify to save current Switch log to NV-RAM. <i>all</i> – Specify to save all configuration settings. If nothing is specified after "save", the Switch will save all.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DES-3528:5#save
Command: save

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

DES-3528:5#
```

reboot


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

Example usage:

To restart the Switch:

```
DES-3528:5#reboot
Command: reboot
Are you sure you want to proceed with the system reboot? (y|n)y
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><i>config</i> – 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><i>system</i> – 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><i>force_agree</i> – 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>
	 <p>NOTE: The serial port baud rate will not be changed by the reset command. It will not be restored to the factory default setting.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3528:5#reset config
Command: reset config
Are users sure to proceed with system reset?(y/n)y
Success.
DES-3528:5#
```

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-3528:5#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-3528:5#logout
```

MODIFY BANNER AND PROMPT COMMANDS

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

Command	Parameters
config command_prompt	[<string 16> username default]
config greeting_message	{default}
show greeting_message	

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

config command prompt	
Purpose	Used to configure the command prompt.
Syntax	config command_prompt [<string 16> username default]
Description	This command is used to change the command prompt.
Parameters	<p><i>string 16</i> – The command prompt can be changed by entering a new name of no more that 16 characters.</p> <p><i>username</i> – The command prompt will be changed to the login username.</p> <p><i>default</i> – The command prompt will reset to factory default command prompt.</p>
Restrictions	<p>Only Administrator and Operator-level users can issue this command. Other restrictions include:</p> <ul style="list-style-type: none"> 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.

Example usage:

To modify the command prompt to “AtYourService”:

```
DES-3528:5#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:admin5#
```

config greeting _message

Purpose	Used to configure the login banner (greeting message).												
Syntax	config greeting _message {default}												
Description	This command is used to modify the login banner (greeting message).												
Parameters	<p><i>default</i> – If the user enters <i>default</i> to the modify banner command, then the banner will be reset to the original factory banner.</p> <p>To open the Banner Editor, click <i>enter</i> 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 and Operator-level users can issue this command. Other restrictions include:</p> <ul style="list-style-type: none"> • 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. • The capacity of the banner is 6*80. 6 Lines and 80 characters per line. • Ctrl+W will only save the modified banner in the DRAM. Users need to type the “save” command to save it into FLASH. • Only valid in threshold level. 												

Example usage:

To modify the banner:

```
DES-3528:5# config greeting_message
Command: config greeting_message

Greeting Messages Editor
=====
                        DES-3528 Fast Ethernet Switch
                        Command Line Interface

                        Firmware: Build 2.00.B031
                        Copyright(C) 2009 D-Link Corporation. All rights reserved.
=====

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

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-3528:5#show greeting_message
Command: show greeting_message

=====
                DES-3528 Fast Ethernet Switch
                Command Line Interface

                Firmware: Build 2.00.B031
                Copyright(C) 2009 D-Link Corporation. All rights reserved.
=====

DES-3528:5#
```

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

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

config ports

Purpose	Used to configure the Switch's port settings.
Syntax	config ports [<portlist> all] {medium_type[fiber copper]}{speed [auto 10_half 10_full 100_half 100_full 1000_full {master slave}] flow_control [enable disable] learning [enable disable] state [enable disable] [description <desc 1-32> clear_description 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><i>all</i> – Configure all ports on the Switch.</p> <p><portlist> – Specifies a port or range of ports to be configured.</p> <p><i>speed</i> – 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"> • <i>auto</i> – Enables auto-negotiation for the specified range of ports. • <i>[10 100 1000]</i> – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 and cannot be set to slower speeds. When setting port speed to 1000_full, user should specify master or slave mode for 1000 base TX interface, and leave the 1000_full without any master or slave setting for other interfaces. • <i>[half full]</i> – Configures the specified range of ports as either full-duplex or half-duplex. <p><i>flow_control [enable disable]</i> – Enable or disable flow control for the specified ports.</p> <p><i>learning [enable disable]</i> – Enables or disables the MAC address learning on the specified range of ports.</p> <p><i>medium_type</i> – Specify the medium type while the configured ports are combo ports. It's an optional parameter for configuring medium type combo ports. For no combo ports, user does not need to specify medium_type in the commands.</p> <p><i>state [enable disable]</i> – Enables or disables the specified range of ports.</p> <p><i>description</i> – Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.</p> <p><i>clear description</i> – To clear the description.</p> <p><i>mdix [auto normal cross]</i> – MDIX mode can be specified as <i>auto</i>, <i>normal</i>, or <i>cross</i>. If set to normal state, the port is in MDIX mode and can be connected to a port on an end node, such as a server or PC, using a straight-through cable. If set to cross state, the port is in MDI mode, and can be connected to a port on another switch or hub that uses MDI-X ports</p>

config ports

through a straight-through cable. If set to auto state, the ports can be connected to any connections by using straight-through or cross-over cable. The ports make the necessary adjustments to accommodate either cable for correct operation.

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

Example usage:

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

```
DES-3528:5# config ports 1-3 speed 10_full learning enable state enable flow_control enable
```

```
Command: config ports 1-3 speed 10_full learning enable state enable flow_control enable
```

```
Success.
```

```
DES-3528:5#
```

show ports

Purpose Used to display the current configuration of a range of ports.

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

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

Parameters

- <portlist> – Specifies a port or range of ports to be displayed.
- description* – Adding this parameter to the **show ports** command indicates that a previously entered port description will be included in the display.
- err_disabled* – Use this to list disabled ports including connection status and reason for being disabled.
- details* – Use this to show the detail information of ports.

Restrictions None.

Example usage:

To display the configuration of all ports on a switch:

```
DES-3528:5#show ports
Command: show ports
```

Port	State/ MDIX	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1	Enabled Auto	Auto/Disabled	Link Down	Enabled
2	Enabled Auto	Auto/Disabled	Link Down	Enabled
3	Enabled Auto	Auto/Disabled	Link Down	Enabled
4	Enabled Auto	Auto/Disabled	Link Down	Enabled
5	Enabled Auto	Auto/Disabled	Link Down	Enabled
6	Enabled Auto	Auto/Disabled	Link Down	Enabled
7	Enabled Auto	Auto/Disabled	Link Down	Enabled
8	Enabled Auto	Auto/Disabled	Link Down	Enabled
9	Enabled Auto	Auto/Disabled	Link Down	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-3528:5#show ports description
Command: show ports description
```

Port	State/ MDIX	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1	Enabled Auto Description:	Auto/Disabled	Link Down	Enabled
2	Enabled Auto Description:	Auto/Disabled	Link Down	Enabled
3	Enabled Auto Description:	Auto/Disabled	Link Down	Enabled
4	Enabled Auto Description:	Auto/Disabled	Link Down	Enabled
5	Enabled Auto Description:	Auto/Disabled	Link Down	Enabled
6	Enabled Auto Description:	Auto/Disabled	Link Down	Enabled

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

Example usage:

To display disabled ports including connection status and reason for being disabled on a standalone switch:


```
DES-3552:5#show ports err_disabled
Command: show ports err_disabled

Port      Port      Connection Status      Reason
-----  -
DES-3552:5#
```

Example usage:

To display detail information of ports on the Switch:

```
Port : 1
-----
Port Status           : Link Down
Description           :
HardWare Type        : Fast Ethernet
MAC Address           : 00-21-91-AF-EA-00
Bandwidth             : 100000Kbit
Auto-Negotiation     : Enabled
Duplex Mode          : Full Duplex
Flow Control         : Disabled
MDI                   : Auto
Address Learning     : Enabled
SFP Module Vendor    :
SFP Module Part Number :
Loopback Mode        :
Last clear of Counter : 5 hours 43 mins ago
BPDU Hardware Filtering Mode: Disabled
Queuing Strategy     : FIFO
TX Load              : 0/100, 0bits/sec, 0packets/sec
RX Load              : 0/100, 0bits/sec, 0packets/sec
TX Counter
  Excessive Deferrals : 0      Late Collisions : 0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

enable jumbo_frame

Purpose	Used to enable the jumbo frame function on the Switch.
Syntax	enable jumbo_frame
Description	This command will allow ethernet frames larger than 1536 bytes to be processed by the Switch. The maximum size of the jumbo frame may not exceed 9220 Bytes tagged.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enabled the jambo frame:

```
DES-3528:5# enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 9216 bytes.
Success.

DES-3528:5#
```

disable jumbo_frame

Purpose	Used to disable the jumbo frame function on the Switch.
Syntax	disable jumbo_frame
Description	This command will disable the jumbo frame function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the jumbo frame:

```
DES-3528:5# disable jumbo_frame
Command: disable jumbo_frame

Success.

DES-3528:5#
```

show jumbo_frame

Purpose	Used to show the status of the jumbo frame function on the Switch.
Syntax	show jumbo_frame
Description	This command will show the status of the jumbo frame function on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the jumbo frame status currently configured on the Switch:

```
DES-3528:5# show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State : Disabled
Maximum Frame Size : 1536 Bytes

DES-3528:5#
```

PORT SECURITY COMMANDS

The Switch's 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	[<portlist> all] {admin_state [enable disable] max_learning_addr <max_lock_no 0-64> lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]}(1)
delete port_security_entry	vlan_name <vlan_name 32> mac_address <macaddr> port <port>
clear port_security_entry	port <portlist>
show port_security	{ports <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 [<portlist> all] {admin_state [enable disable] max_learning_addr <max_lock_no 0-64> lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]}(1)
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <portlist> are affected.
Parameters	<p><i>portlist</i> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Configure port security for all ports on the Switch.</p> <p><i>admin_state [enable disable]</i> – Enable or disable port security for the listed ports.</p> <p><i>max_learning_addr <max_lock_no 0-64></i> – Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p><i>lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]</i> – Indicates the method of locking addresses. The user has three choices:</p> <ul style="list-style-type: none"> ▪ <i>Permanent</i> – The locked addresses will not age out after the aging timer expires. ▪ <i>DeleteOnTimeout</i> – The locked addresses will age out after the aging timer expires. ▪ <i>DeleteOnReset</i> – The locked addresses will not age out until the Switch has been reset.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port security:

```
DES-3528:5#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-3528:5#
```

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

Example usage:

To delete a port security entry:

```
DES-3528:5#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-3528:5#
```

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 port <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	<i><portlist></i> – Specifies a port or port range to clear.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear a port security entry by port:

```
DES-3528:5# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DES-3528:5#
```

show port_security

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

Example usage:

To display the port security configuration:

```
DES-3528:5#show port_security ports 1-5
Command: show port_security ports 1-5

Port_security Trap/Log : Disabled

  Port      Admin State  Max. Learning Addr.  Lock Address Mode
  ----      -
  1         Disabled    1                    DeleteOnReset
  2         Disabled    1                    DeleteOnReset
  3         Disabled    1                    DeleteOnReset
  4         Disabled    1                    DeleteOnReset
  5         Disabled    1                    DeleteOnReset

DES-3552:5#
```

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 and 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 and Operator-level users can issue this command.

Example usage:

To enable the port security trap log setting:

```
DES-3528:5#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3528:5#
```

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 enable and 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 and Operator-level users can issue this command.

Example usage:

To disable the port security trap log setting:

```
DES-3528:5#disable port_security trap_log
Command: disable port_security trap_log

Success.

DES-3528:5#
```

STACKING COMMANDS

The stacking configuration commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config box_priority current_box_id	<value 1-8> priority <value 1-63>
config box_id current_box_id	<value 1-8> new_box_id [auto 1 2 3 4 5 6 7 8]
show stack_information	
config stacking mode	[disable enable]
show stacking mode	

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

config box_priority

Purpose	Used to configure box priority so as to determine which box (switch) becomes the master. A lower number denotes a higher priority.
Syntax	config box_priority current_box_id <value 1-8> priority <value 1-63>
Description	This command is used to configure the box (switch) priority.
Parameters	<i>current_box_id <value 1-8></i> – Identifies the Switch being configured. Range is 1 to 8. <i>priority <value 1-63></i> – Assigns a priority value to the box. A Lower number denotes a higher priority. The valid priority range is 1 to 63.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To configure box priority:

```
DES-3528:5#config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

DES-3528:5#
```

config box_id

Purpose	Used to configure box ID. Users can use this command to reassign box IDs.
Syntax	config box_id current_box_id <value 1-8> new_box_id [auto 1 2 3 4 5 6 7 8]
Description	This command is used to assign box IDs to switches in a stack.
Parameters	<i>current_box_id</i> – Identifies the Switch being configured. Range is 1 to 8. <i>new_box_id</i> – The new ID being assigned to the Switch (box). Range is 1 to 8. <ul style="list-style-type: none"> <i>auto</i> – Allows the box ID to be assigned automatically.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To change a box ID:

```
DES-3528:5#config box_id current_box_id 1 new_box_id 2
Command: config box_id current_box_id 1 new_box_id 2

Success.

DES-3528:5#
```

show stack_information

Purpose	Used to display the stack information table.
Syntax	show stack_information
Description	This command display stack information.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To display stack information:

```
DES-3528:5# show stack_information
Command: show stack_information

Topology      :Duplex_Chain
My Box ID     :1
Master ID     :1
BK Master ID  :2
Box Count     :2

Box User          Prio-      Prom      Runtime  H/W
ID  Set  Type      Exist rity      MAC      version  version  version
---  ---  -
  1 Auto DES-3528  Exist 20  00-00-00-00-01-96  1.00.B007  2.00.B025  A2
  2 Auto DES-3528P  Exist 32  00-01-03-04-04-04  1.00.B007  2.00.B025  A1
  3   -  DES-3528P   No
  4   -  NOT_EXIST   No
  5   -  NOT_EXIST   No
  6   -  NOT_EXIST   No
  7   -  NOT_EXIST   No
  8   -  NOT_EXIST   No

DES-3528:5#
```


config stacking mode

Purpose	Used to configure the stacking mode.
Syntax	config stacking mode [disable enable]
Description	This command will enable or disable the stacking mode for the switch. When enabled, the last two ports on the rear of the switch will be enabled for stacking.
Parameters	<i>enable</i> / <i>disable</i> – Use these parameters to enable or disable the stacking mode for the switch. Once this command is executed, it will cause the switch to reboot. Before configuring the stacking mode of a switch to disable status, the switch must be physically removed from the stacking switches.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To disable the stacking mode:

```
DES-3528:5#config stacking mode disable
Command: config stacking mode disable

Change Box bootmode may cause devices work restart, still continue? (y/n)y
```

show stacking mode

Purpose	Used to view the current stacking mode.
Syntax	show stacking mode
Description	This command will display whether the current stacking mode is enabled or disabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To view the current stacking mode:

```
DES-3528:5#show stacking mode
Command: show stacking mode

Stacking mode : Enabled

DES-3528:5#
```

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, AuthNoPriv or AuthPriv
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	<user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > sha <auth_password 8-20>] priv [none des <priv_password 8-16>] by_key auth [md5 <auth_key 32-32> sha <auth_key 40-40>] priv [none des <priv_key 32-32>]]}
delete snmp user	<user_name 32>
show snmp user	
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	[all ipaddr<ipaddr> network<network_address>]
show trusted_host	{<network_address>}
enable snmp traps	
enable snmp authenticate_traps	
show snmp traps	
disable snmp traps	
disable snmp authenticate_traps	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable snmp	
disable snmp	

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 <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> sha <auth_password 8-20>] priv [none des <priv_password 8-16>] by_key auth [md5 <auth_key 32-32> sha <auth_key 40-40>] priv [none des <priv_key 32-32>]]}
Description	This command creates a new SNMP user and adds the user to an SNMP group that is also created by this command. SNMP ensures: Message integrity – Ensures that packets have not been tampered with during transit. Authentication – Determines if an SNMP message is from a valid source. Encryption – Scrambles the contents of messages to prevent it from being viewed by an unauthorized source.
Parameters	<p><user_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 a encryption key for authentication and privacy. The key is defined by specifying the key in hex form below. 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

create snmp user

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.

priv – Adding the *priv* (privacy) parameter will allow for encryption in addition to the authentication algorithm for higher security. The user may choose:

des – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using:

- *<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-3528:5#create snmp user dlink default encrypted by_password auth md5 canadian priv
none
Command: create snmp user dlink default encrypted by_password auth md5 canadian priv
none
Success.
DES-3528:5#
```

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 <user_name 32>

Description

This command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.

Parameters

<user_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-3528:5#delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-3528:5#
```

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 displays 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-3528:5#show snmp user
Command: show snmp user

Username      Group Name      VerAuthPriv
-----      -
initial       initial         V3 NoneNone
Total Entries: 1

DES-3528:5#
```

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 assigns 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> <ul style="list-style-type: none"> • <i>included</i> – Include this object in the list of objects that an SNMP manager can access. • <i>excluded</i> – Exclude this object from the list of objects that an SNMP manager can access.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP view:

```
DES-3528:5#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-3528:5#
```

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><i><view_name 32></i> – An alphanumeric string of up to 32 characters that identifies the SNMP view to be deleted.</p> <p><i>all</i> – Specifies that all of the SNMP views on the Switch will be deleted.</p> <p><i><oid></i> – 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-3528:5#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-3528:5#
```

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 displays an SNMP view previously created on the Switch.
Parameters	<i><view_name 32></i> – 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-3528:5#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name      Subtree              View Type
-----
ReadView       1                    Included
WriteView      1                    Included
NotifyView     1.3.6                Included
restricted     1.3.6.1.2.1.1       Included
restricted     1.3.6.1.2.1.11      Included
restricted     1.3.6.1.6.3.10.2.1  Included
restricted     1.3.6.1.6.3.11.2.1  Included
restricted     1.3.6.1.6.3.15.1.1  Included
CommunityView  1                    Included
CommunityView  1.3.6.1.6.3          Excluded
CommunityView  1.3.6.1.6.3.1       Included

Total Entries: 11

DES-3528:5#

```

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 Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent. An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community. <i>read_write</i> or <i>read_only</i> 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	<i><community_string 32></i> – 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. <i>view <view_name 32></i> – 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. <i>read_only</i> – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch. <i>read_write</i> – 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	Only Administrator-level users can issue this command.

Example usage:

To create the SNMP community string "dlink:"

```
DES-3528:5#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DES-3528:5#
```

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-3528:5#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-3528:5#
```

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-3528:5#show snmp community
Command: show snmp community

SNMP Community Table

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

Total Entries: 3

DES-3528:5#
```

config snmp engineID

Purpose	Used to configure a name for the SNMP engine on the Switch.
Syntax	config snmp engineID <snmp_engineID 10-64>
Description	This command configures a name for the SNMP engine on the Switch.
Parameters	<config snmp_engineID> – 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-3528:5#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DES-3528:5#
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the Switch.
Syntax	show snmp engineID
Description	This command displays 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-3528:5#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DES-3528:5#
```

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 creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	<p><i><groupname 32></i> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p><i>v1</i> – 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><i>v2c</i> – 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><i>v3</i> – 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> <ul style="list-style-type: none"> • Message integrity – Ensures that packets have not been tampered with during transit. • Authentication – Determines if an SNMP message is from a valid source. • Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source. <p><i>noauth_nopriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – 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><i>auth_priv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manager will be encrypted.</p> <p><i>read_view</i> – Specifies that the SNMP group being created can request SNMP messages.</p> <p><i>write_view</i> – Specifies that the SNMP group being created has write privileges.</p> <p><i>notify_view</i> – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent.</p> <p><i><view_name 32></i> – 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	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP group named "sg1":

```
DES-3528:5#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-3528:5#
```

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-3528:5#delete snmp group sg1
```

```
Command: delete snmp group sg1
```

```
Success.
```

```
DES-3528:5#
```

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 displays 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-3528:5#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-3528:5#
```

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 creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<p><i><ipaddr></i> – The IP address of the remote management station that will serve as the SNMP host for the Switch.</p> <p><i>v1</i> – 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><i>v2c</i> – 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><i>v3</i> – 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> <ul style="list-style-type: none"> • Message integrity – ensures that packets have not been tampered with during transit. • Authentication – determines if an SNMP message is from a valid source. • Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source. <p><i>noauth_nopriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – 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><i>auth_priv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manager will be encrypted.</p> <p><i><auth_string 32></i> – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-3528:5#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-3528:5#
```

delete snmp host

Purpose	Used to remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	delete snmp host <ipaddr>
Description	This command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<i><ipaddr></i> – 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-3528:5#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DES-3528:5#
```

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-3528:5#show snmp host
Command: show snmp host

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

Total Entries: 2

DES-3528:5#
```

create trusted_host

Purpose	Used to create the trusted host.
Syntax	create trusted_host [<ipaddr> network <network_address>]
Description	This command creates the trusted host. The Switch allows users to specify up to four 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> – IP address and netmask of the trusted host to be created.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the trusted host:

```
DES-3528:5#create trusted_host 10.62.32.1
Command: create trusted_host 10.62.32.1

Success.
```

create trusted_host network

Purpose	Used to create the trusted host.
Syntax	create trusted_host network <network_address>
Description	This command is used to create the trusted host.
Parameters	<network_address> – IP address and netmask of the trusted host to be created.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the trusted host network.

```
DES-3528:5#create trusted_host network 10.62.32.1/16
Command: create trusted_host network 10.62.32.1/16

Success.
```

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 a list of trusted hosts entered on the Switch using the create trusted_host command above.
Parameters	<network_address> – the network address to show
Restrictions	None.

Example Usage:

To display the list of trust hosts:

```
DES-3528: 5#show trusted_host
Command: show trusted_host

Management Stations

IP Address/Netmask
-----
10.62.32.1/32
10.62.32.1/16

Total Entries: 2
```

delete trusted_host ipaddr

Purpose	Used to delete a trusted host entry made using the create trusted_host command above.
Syntax	delete trusted_host ipaddr <ipaddr>
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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a trusted host with an IP address 10.62.32.1:

```
DES-3528:5#delete trusted_host ipaddr 10.62.32.1
Command: delete trusted_host ipaddr 10.62.32.1

Success.
```

delete trusted_host network

Purpose	Used to delete a trusted host entry made using the create trusted_host network command above.
Syntax	delete trusted_host network <network_address>
Description	This command is used to delete a trusted host entry made using the create trusted_host network command above.
Parameters	<network_address> – IP address and netmask of the trusted host network.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a trusted host network IP address 10.62.31.1/16:

```
DES-3528:5#delete trusted_host network 10.62.32.1/16
Command: delete trusted_host network 10.62.32.1/16

Success.
```

delete trusted_host all

Purpose	Used to delete all trusted host entries made using the create trusted_host ipaddr and create trusted_host network commands above.
Syntax	delete trusted_host all
Description	This command is used to delete all trusted host entries made using the create trusted_host ipaddr and create trusted_host network commands above.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete all trusted host entries:

```
DES-3528: 5#delete trusted_host all
Command: delete trusted_host all

Success.
```


enable snmp traps

Purpose	Used to enable SNMP trap support.
Syntax	enable snmp traps
Description	This command is used to enable SNMP trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable SNMP trap support on the Switch:

```
DES-3528:5#enable snmp traps
Command: enable snmp traps

Success.

DES-3528:5#
```

enable snmp authenticate_traps

Purpose	Used to enable SNMP authentication trap support.
Syntax	enable snmp authenticate_traps
Description	This command is used to enable SNMP authentication trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To turn on SNMP authentication trap support:

```
DES-3528:5#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DES-3528:5#
```

show snmp traps

Purpose	Used to show SNMP trap support on the Switch .
Syntax	show snmp traps
Description	This command is used to view the SNMP trap support status currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DES-3528:5#show snmp traps
Command: show snmp traps

SNMP Traps           : Enabled
Authenticate Trap    : Enabled

DES-3528:5#
```

disable snmp traps

Purpose	Used to disable SNMP trap support on the Switch.
Syntax	disable snmp traps
Description	This command is used to disable SNMP trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DES-3528:5#disable snmp traps
Command: disable snmp traps

Success.

DES-3528:5#
```

disable snmp authenticate_traps

Purpose	Used to disable SNMP authentication trap support.
Syntax	disable snmp authenticate_traps
Description	This command is used to disable SNMP authentication support on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the SNMP authentication trap support:

```
DES-3528:5#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DES-3528:5#
```

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 255 character can be used.
Parameters	<sw_contact> – A maximum of 255 characters is allowed. A NULL string is accepted if there is no contact.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DES-3528:5#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DES-3528:5#
```

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 255 characters can be used.
Parameters	<sw_location> – A maximum of 255 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DES-3528:5#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3528:5#
```

config snmp system_name

Purpose	Used to configure the name for the Switch.
Syntax	config snmp system_name <sw_name>
Description	This command configures the name of the Switch.
Parameters	<sw_name> – A maximum of 255 characters is allowed. A NULL string is accepted if no name is desired.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Switch name for “DES-3526 Switch”:

```
DES-3528:5#config snmp system_name DES-3526 Switch
Command: config snmp system_name DES-3526 Switch

Success.

DES-3528:5#
```

enable snmp

Purpose	Used to enable the SNMP interface access function.
Syntax	enable snmp
Description	This command is used to enable the SNMP function.
Parameters	None
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable snmp on the Switch:

```
DES-3528:5#enable snmp
Command: enable snmp

Success.

DES-3528:5#
```

disable snmp

Purpose	Used to disable the SNMP interface access function.
Syntax	disable snmp
Description	This command is used to disable the SNMP function. When the SNMP function is disabled, the network manager will not be able to access SNMP MIB objects. The device will not send traps or notifications to the network manager either.
Parameters	None
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable SNMP on the Switch:

```
DES-3528:5#disable snmp
Command: disable snmp

Success.

DES-3528:5#
```

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> <path_filename 64> {image_id <int 1-2>} {unit [all <unitid 1-8>]} cfg_fromTFTP <ipaddr> <path_filename 64> {[<config_id 1-2> increment]}]
config firmware	{unit <unit_id 1-8>} image_id <int 1-2> [delete boot_up]
show firmware_information	
show config	[current_config config_in_nvram <config_id 1-2> information]
upload	[cfg_toTFTP <ipaddr> <path_filename 64> { <config_id 1-2>} log_toTFTP <ipaddr> <path_filename 64> attack_log_toTFTP <ipaddr> <path_filename 64> {unit <unit_id 1-8>}]
enable autoconfig	
disable autoconfig	
show autoconfig	
config configuration	<config_id 1-2>[boot_up delete active]
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}

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> <path_filename 64> {image_id <int 1-2>} {unit [all <unitid 1-8>]} cfg_fromTFTP <ipaddr> <path_filename 64> {[<config_id 1-2> increment]}]
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	<p><i>firmware_fromTFTP</i> – Download and install new firmware on the Switch from a TFTP server.</p> <p><i>cfg_fromTFTP</i> – Download a switch configuration file from a TFTP server.</p> <p><i><ipaddr></i> – The IP address of the TFTP server.</p> <p><i><path_filename></i> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3528.had.</p> <p><i>image_id <int 1-2></i> – 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><i>unit</i> - Specifies which unit(s) on the stacking system can download and install new firmware from a TFTP server. If it is not specified, it refers to all the units. For example, <i>unit 1-3</i>.</p> <p><i>config_id</i> - Specifies configuration ID in the system; If it is not specified, it refers to the boot up configuration ID.</p> <p><i>increment</i> – 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-3528:5#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.

DES-3528:5#
DES-3528:5##-----
DES-3528:5##                DES-3528 Configuration
DES-3528:5##
DES-3528:5##                Firmware: Build 2.00.B033
DES-3528:5##                Copyright(C) 2009 D-Link Corporation. All rights reserved.
DES-3528:5##-----
DES-3528:5#
DES-3528:5#
DES-3528:5## BASIC
DES-3528:5#
DES-3528:5#config serial_port baud_rate 115200 auto_logout 10_minutes
Command: config serial_port baud_rate 115200 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-3528” appears followed by the command prompt.

```
DES-3528:5#disable authen_policy
Command: disable authen_policy

Success.

DES-3528:5#
DES-3528:5##-----
DES-3528:5##                End of configuration file for DES-3528
DES-3528:5##-----
DES-3528:5#
```

config firmware	
Purpose	Used to configure the firmware section as a boot up section, or to delete the firmware section
Syntax	config firmware {unit <unit_id 1-8>} image_id <int 1-2> [delete boot_up]
Description	This command is used to configure the firmware section. The user may choose to remove the firmware section or use it as a boot up section.
Parameters	<p><i>unit</i> – Specifies the unit on the stacking system. If it is not specified, it refers to the master unit.</p> <p><i>image_id</i> – Specifies the working section. The Switch can hold two firmware versions for the user to select from, which are specified by image ID.</p> <p><i>delete</i> – Entering this parameter will delete the specified firmware section.</p> <p><i>boot_up</i> – Entering this parameter will specify the firmware image ID as a boot up section.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure firmware image 1 as a boot up section:

```
DES-3528:5# config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DES-3528:5#
```

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-3528:5#show firmware information
Command: show firmware information

ID  Version      Size(B)      Update Time                From                        User
--  -
 1  1.00-T003    2103164     2000/01/02 01:21:21          10.90.90.11(R)           Anonymous
*2  1.03.B008    2317149     0 days 00:00:00          Serial Port(Prom)       Unknown

'*' means boot up firmware
(R) means firmware update through Serial Port(RS232)
(T) means firmware update through TELNET
(S) means firmware update through SNMP
(W) means firmware update through WEB
(SSH) means firmware update through SSH
(SIM) means firmware update through Single IP Management

DES-3528:5#
```

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 <config_id 1-2> information]																																																						
Description	<p>This command is used to display all the configuration settings that are saved to NV RAM 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>1. Basic (serial port, Telnet and web management status)</td> <td>28. PPPoE</td> </tr> <tr> <td>2. storm control</td> <td>29. MAC address table notification</td> </tr> <tr> <td>3. loop detect</td> <td>30. STP</td> </tr> <tr> <td>4. SIM</td> <td>31. BPDU protection</td> </tr> <tr> <td>5. syslog</td> <td>32. safeguard</td> </tr> <tr> <td>6. QoS</td> <td>33. SSH</td> </tr> <tr> <td>7. port mirroring</td> <td>34. SNTP</td> </tr> <tr> <td>8. traffic segmentation</td> <td>35. LACP</td> </tr> <tr> <td>9. SSL</td> <td>36. IP</td> </tr> <tr> <td>10. port</td> <td>37. WAC</td> </tr> <tr> <td>11. SFLOW</td> <td>38. CFM</td> </tr> <tr> <td>12. OAM</td> <td>39. JWAC</td> </tr> <tr> <td>13. port lock</td> <td>40. LLDP</td> </tr> <tr> <td>14. SNMPv3</td> <td>41. IGMP snooping</td> </tr> <tr> <td>15. management (SNMP traps RMON)</td> <td>42. MBA</td> </tr> <tr> <td>16. vlan</td> <td>43. MLD vlan</td> </tr> <tr> <td>17. Q-in-Q</td> <td>44. multicast</td> </tr> <tr> <td>18. RSPAN</td> <td>45. multicast authentication</td> </tr> <tr> <td>19. 802.1x</td> <td>46. igmp snooping</td> </tr> <tr> <td>20. ACL</td> <td>47. mld snooping</td> </tr> <tr> <td>21. POE</td> <td>48. access authentication control (TACACS etc.)</td> </tr> <tr> <td>22. FDB (forwarding data base)</td> <td>49. ARP</td> </tr> <tr> <td>23. address binding</td> <td>50. route</td> </tr> <tr> <td>24. net bios</td> <td>51. dns relay</td> </tr> <tr> <td>25. dhcp server screening</td> <td>52. dhcp server</td> </tr> <tr> <td>26. sRED</td> <td>53. dhcp relay</td> </tr> <tr> <td>27. ARP spoofing prevention</td> <td></td> </tr> </table>	1. Basic (serial port, Telnet and web management status)	28. PPPoE	2. storm control	29. MAC address table notification	3. loop detect	30. STP	4. SIM	31. BPDU protection	5. syslog	32. safeguard	6. QoS	33. SSH	7. port mirroring	34. SNTP	8. traffic segmentation	35. LACP	9. SSL	36. IP	10. port	37. WAC	11. SFLOW	38. CFM	12. OAM	39. JWAC	13. port lock	40. LLDP	14. SNMPv3	41. IGMP snooping	15. management (SNMP traps RMON)	42. MBA	16. vlan	43. MLD vlan	17. Q-in-Q	44. multicast	18. RSPAN	45. multicast authentication	19. 802.1x	46. igmp snooping	20. ACL	47. mld snooping	21. POE	48. access authentication control (TACACS etc.)	22. FDB (forwarding data base)	49. ARP	23. address binding	50. route	24. net bios	51. dns relay	25. dhcp server screening	52. dhcp server	26. sRED	53. dhcp relay	27. ARP spoofing prevention	
1. Basic (serial port, Telnet and web management status)	28. PPPoE																																																						
2. storm control	29. MAC address table notification																																																						
3. loop detect	30. STP																																																						
4. SIM	31. BPDU protection																																																						
5. syslog	32. safeguard																																																						
6. QoS	33. SSH																																																						
7. port mirroring	34. SNTP																																																						
8. traffic segmentation	35. LACP																																																						
9. SSL	36. IP																																																						
10. port	37. WAC																																																						
11. SFLOW	38. CFM																																																						
12. OAM	39. JWAC																																																						
13. port lock	40. LLDP																																																						
14. SNMPv3	41. IGMP snooping																																																						
15. management (SNMP traps RMON)	42. MBA																																																						
16. vlan	43. MLD vlan																																																						
17. Q-in-Q	44. multicast																																																						
18. RSPAN	45. multicast authentication																																																						
19. 802.1x	46. igmp snooping																																																						
20. ACL	47. mld snooping																																																						
21. POE	48. access authentication control (TACACS etc.)																																																						
22. FDB (forwarding data base)	49. ARP																																																						
23. address binding	50. route																																																						
24. net bios	51. dns relay																																																						
25. dhcp server screening	52. dhcp server																																																						
26. sRED	53. dhcp relay																																																						
27. ARP spoofing prevention																																																							
Parameters	<p><i>current_config</i> – Entering this parameter will display configurations entered without being saved to NVRAM.</p> <p><i>config_in_NVRAM</i> – Entering this parameter will display configurations entered and saved to NVRAM.</p> <p><i>information</i> – Entering this parameter will display the global information for the configuration settings.</p>																																																						
Restrictions	Only Administrator and Operator-level users can issue this command.																																																						

Example usage:

To view the current configuration settings:


```

DES-3528:5#show config current_config
Command: show config current_config

#-----
#                DES-3528 Configuration
#
#                Firmware: Build 2.00.B031
# Copyright(C) 2009 D-Link Corporation. All rights reserved.
#-----

# STACK

# BASIC

# ACCOUNT LIST
# ACCOUNT END
# PASSWORD ENCRYPTION
disable password encryption
config serial_port auto_logout 10_minutes
enable telnet 23
enable web 80

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 [<i>cfg_toTFTP</i> <ipaddr> <path_filename 64> { <config_id 1-2> } <i>log_toTFTP</i> <ipaddr> <path_filename 64> <i>attack_log_toTFTP</i> <ipaddr> <path_filename 64> {unit <unit_id 1-8> }]
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><i>cfg_toTFTP</i> – Specifies that the Switch's current settings will be uploaded to the TFTP server.</p> <p><i>log_toTFTP</i> – Specifies that the switch history log will be uploaded to the TFTP server.</p> <p><i>attack_log_toTFTP</i> – Specifies that the switch attack log will be uploaded to the TFTP server.</p> <p><<i>ipaddr</i>> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch.</p> <p><i>config_id</i> - Specifies configuration ID in the system; If it is not specified, it refers to the boot up configuration ID.</p> <p><i>unit</i> - Specifies which switch unit's attack log will be uploaded, if it is not specified, it refers to the master unit.</p> <p><<i>path_filename 64</i>> – 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 and Operator-level users can issue this command.

Example usage:

To upload a configuration file:

```
DES-3528:5#upload cfg_toTFTP 10.48.74.121 c:\cfg\log.txt
Command: upload cfg_toTFTP 10.48.74.121 c:\cfg\log.txt

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

DES-3528:5#
```

enable autoconfig

Purpose	Used to activate the autoconfiguration function for the Switch. This will load a previously saved configuration file for current use.
Syntax	enable autoconfig
Description	This command is used to enable autoconfig. 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 autoconfiguration process the previously saved local configuration file present in Switch memory will be loaded. Only Administrator and Operator-level users can issue this command.



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 autoconfiguration on the Switch:

```
DES-3528:5#enable autoconfig
Command: enable autoconfig

Success.

DES-3528:5#
```

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-3528 Fast Ethernet Switch Command Line Interface

Firmware: Build 2.00.B033

Copyright(C) 2009 D-Link Corporation. All rights reserved.

```
DES-3528:5#
DES-3528:5#
DES-3528:5#download configuration 10.41.44.44 c:\cfg\setting.txt
Command: download configuration 10.41.44.44 c:\cfg\setting.txt

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

The very end of the autoconfig process including the logout appears like this:

```
DES-3528:5#disable authen_policy
Command: disable authen_policy

Success.

DES-3528:5#
DES-3528:5##-----
DES-3528:5##                End of configuration file for DES-3528
Saving configurations and logs to NV-RAM..... Done.

*****
* Logout *
*****
```



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 to deactivate autoconfiguration from DHCP.
Syntax	disable autoconfig
Description	This command is used to disable autoconfig. This instructs the Switch not to accept autoconfiguration 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 and Operator-level users can issue this command.

Example usage:

To stop the autoconfiguration function:

```
DES-3528:5#disable autoconfig
Command: disable autoconfig

Success.

DES-3528:5#
```

show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	show autoconfig
Description	This command will list the current status of the autoconfiguration function.
Parameters	None.
Restrictions	None.

Example usage:

```
DES-3528:5#show autoconfig
Command: show autoconfig
Autoconfig State: Disabled.

DES-3528:5#
```

config configuration

Purpose	Used to delete the specific firmware or configure the specific firmware as boot up image.
Syntax	config configuration <config_id 1-2> [boot_up delete active]
Description	This command is used to delete the specific firmware or configure the specific firmware as boot up image.
Parameters	<p><i><config_id 1-2></i> – Specifies the serial number of the indicated configuration.</p> <p><i>boot_up</i> – Specifies the config is boot_up config.</p> <p><i>delete</i> – Delete the configuration.</p> <p><i>active</i> – Active specifies the configuration .</p>
Restrictions	You must have Administrator-level privileges.

Example usage:

To configure the specific configuration as boot up image:

```
DES-3528:5#config configuration 2 boot_up
Command: config configuration 2 boot_up

Success.

DES-3528:4#
```

ping

Purpose	Used to test the connectivity between network devices.
Syntax	ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
Description	This command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then "echo" or return the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters	<p><i><ipaddr></i> - Specifies the IP address of the host.</p> <p><i>times <value 1-255></i> - 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><i>timeout <sec 1-99></i> - 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-3528:5#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-3528:5#
```

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 ports {<portlist>}]
clear counters	{ports <portlist>}
clear log	
show log	{index <value_list> }
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	
show attack_log	{unit <unit_id 1-8>} {index <value_list>}
clear attack_log	{unit <unit_id 1-8>}
config system_severity	[trap log all] [critical warning information]
show system_severity	

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

show packet ports

Purpose	Used to display statistics about the 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 7 of module 2:

```
DES-3528:5#show packet port 2
```

```
Command: show packet port 2
```

```
Port Number : 2
```

```
=====
```

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

Frame Type	Total	Total/sec
RX Bytes	0	0
RX Frames	0	0
TX Bytes	0	0
TX Frames	0	0

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

show error ports

Purpose	Used to display the error statistics for a range of ports.
Syntax	show error ports <portlist>
Description	This command will 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 of module 1:

```
DES-3528:5#show error ports 3
```

```
Command: show error ports 3
```

```
Port Number : 3
```

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

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

show utilization

Purpose	Used to display real-time port and CPU utilization statistics.
Syntax	show utilization [cpu ports {<portlist>}]
Description	This command will display the real-time port and CPU utilization statistics for the Switch.
Parameters	<i>cpu</i> – Entering this parameter will display the current cpu utilization of the Switch. <i>ports</i> – Entering this parameter will display the current port utilization of the Switch. <ul style="list-style-type: none"> ▪ <i><portlist></i> – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the port utilization statistics:


```
DES-3528:5#show utilization ports
Command: show utilization ports
```

Port	TX/sec	RX/sec	Util	Port	TX/sec	RX/sec	Util
1	0	0	0	21	0	0	0
2	0	0	0	22	0	0	0
3	0	0	0	23	0	0	0
4	0	0	0	24	0	0	0
5	0	0	0	25	0	0	0
6	0	0	0	26	0	0	0
7	0	0	0	27	0	0	0
8	0	0	0	28	0	0	0
9	19	0	1				
10	0	0	0				
11	0	0	0				
12	0	0	0				
13	0	0	0				
14	0	0	0				
15	1	19	1				
16	0	0	0				
17	0	0	0				
18	0	0	0				
19	0	0	0				
20	0	0	0				

```

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

```

To display the current CPU utilization:

```
DES-3528:5#show utilization cpu
Command: show utilization cpu

CPU utilization :
-----
Five seconds - 15% One minute - 25%Five minutes - 14%

DES-3528:5#
```

clear counters

Purpose	Used to clear the Switch's statistics counters.
Syntax	clear counters {ports <portlist>}
Description	This command will 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 and Operator-level users can issue this command.

Example usage:

To clear the counters:

```
DES-3528:5#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

DES-3528:5#
```

clear log

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

Example usage:

To clear the log information:

```
DES-3528:5#clear log
Command: clear log

Success.

DES-3528:5#
```

show log

Purpose	Used to display the Switch's history log.
Syntax	show log {index <value_list>}
Description	This command will display the contents of the Switch's history log.
Parameters	<i>index <value_list></i> – This parameter specifies the range of log index to show. For example, show log index 1-5 will display the history log from 1 to 5. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.

Example usage:

To display the Switch's history log:

```
DES-3528:5#show log index 1-5
Command: show log index 1-5

Index      Time                Log Text
-----
5          00000 days 00:01:09  Successful login through Console (Username: Anonymous)
4          00000 days 00:00:14  System started up
3          00000 days 00:00:06  Port 1 link up, 100Mbps FULL duplex
2          00000 days 00:00:01  Spanning Tree Protocol is disabled
1          00000 days 00:06:31  Configuration saved to flash (Username: Anonymous)

DES-3528:5#
```



NOTE: For detailed information regarding Log entries that will appear in this window, please refer to Appendix C at the back of the **xStack DES-3528 Layer 2 Stackable Fast Ethernet Managed Switch User Manual**.

enable syslog

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

Example usage:

To the Syslog function on the Switch:

```
DES-3528:5#enable syslog
Command: enable syslog
Success.
DES-3528:5#
```

disable syslog

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

Example usage:

To disable the syslog function on the Switch:

```
DES-3528:5#disable syslog
Command: disable syslog
Success.
DES-3528:5#
```

show syslog

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

Example usage:

To display the current status of the syslog function:

```
DES-3528:5#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-3528:5#
```

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><i><index 1-4></i> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p><i>ipaddress <ipaddr></i> – Specifies the IP address of the remote host where syslog messages will be sent.</p> <p><i>severity</i> – 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="0"> <thead> <tr> <th>Numerical Code</th> <th>Severity</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency: system is unusable</td> <td></td> <td></td> </tr> <tr> <td>1</td> <td>Alert: action must be taken immediately</td> <td></td> <td></td> </tr> <tr> <td>2</td> <td>Critical: critical conditions</td> <td></td> <td></td> </tr> <tr> <td>3</td> <td>Error: error conditions</td> <td></td> <td></td> </tr> <tr> <td>4</td> <td>Warning: warning conditions</td> <td></td> <td></td> </tr> <tr> <td>5</td> <td>Notice: normal but significant condition</td> <td></td> <td></td> </tr> <tr> <td>6</td> <td>Informational: informational messages</td> <td></td> <td></td> </tr> <tr> <td>7</td> <td>Debug: debug-level messages</td> <td></td> <td></td> </tr> </tbody> </table> <table border="0"> <thead> <tr> <th>Numerical Code</th> <th>Facility</th> <th>Numerical Code</th> <th>Facility</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>kernel messages</td> <td>12</td> <td>NTP subsystem</td> </tr> <tr> <td>1</td> <td>user-level messages</td> <td>13</td> <td>log audit</td> </tr> <tr> <td>2</td> <td>mail system</td> <td>14</td> <td>log alert</td> </tr> <tr> <td>3</td> <td>system daemons</td> <td>15</td> <td>clock daemon</td> </tr> <tr> <td>4</td> <td>security/authorization messages</td> <td>16</td> <td>local use 0 (local0)</td> </tr> <tr> <td>5</td> <td>messages generated internally by syslog</td> <td>17</td> <td>local use 1 (local1)</td> </tr> <tr> <td>6</td> <td>line printer subsystem</td> <td>18</td> <td>local use 2 (local2)</td> </tr> <tr> <td>7</td> <td>network news subsystem</td> <td>19</td> <td>local use 3 (local3)</td> </tr> <tr> <td>8</td> <td>UUCP subsystem</td> <td>20</td> <td>local use 4 (local4)</td> </tr> <tr> <td>9</td> <td>clock daemon</td> <td>21</td> <td>local use 5 (local5)</td> </tr> <tr> <td>10</td> <td>security/authorization messages</td> <td>22</td> <td>local use 6 (local6)</td> </tr> <tr> <td>11</td> <td>FTP daemon</td> <td>23</td> <td>local use 7 (local7)</td> </tr> </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	Facility	0	kernel messages	12	NTP subsystem	1	user-level messages	13	log audit	2	mail system	14	log alert	3	system daemons	15	clock daemon	4	security/authorization messages	16	local use 0 (local0)	5	messages generated internally by syslog	17	local use 1 (local1)	6	line printer subsystem	18	local use 2 (local2)	7	network news subsystem	19	local use 3 (local3)	8	UUCP subsystem	20	local use 4 (local4)	9	clock daemon	21	local use 5 (local5)	10	security/authorization messages	22	local use 6 (local6)	11	FTP daemon	23	local use 7 (local7)
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	Facility																																																																																								
0	kernel messages	12	NTP subsystem																																																																																								
1	user-level messages	13	log audit																																																																																								
2	mail system	14	log alert																																																																																								
3	system daemons	15	clock daemon																																																																																								
4	security/authorization messages	16	local use 0 (local0)																																																																																								
5	messages generated internally by syslog	17	local use 1 (local1)																																																																																								
6	line printer subsystem	18	local use 2 (local2)																																																																																								
7	network news subsystem	19	local use 3 (local3)																																																																																								
8	UUCP subsystem	20	local use 4 (local4)																																																																																								
9	clock daemon	21	local use 5 (local5)																																																																																								
10	security/authorization messages	22	local use 6 (local6)																																																																																								
11	FTP daemon	23	local use 7 (local7)																																																																																								

create syslog host

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.

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

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

Example usage:

To create a Syslog host:

```
DES-3528:5#create syslog host 1 severity all facility local0 ipaddress 1.1.1.1
```

```
Command: create syslog host 1 severity all facility local0 ipaddress 1.1.1.1
```

Success.

```
DES-3528:5#
```

config syslog host

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 <index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.

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

severity – Severity level indicator. These are described in the following:

Bold font indicates that the corresponding severity level is currently supported on the Switch.

Numerical	Severity
Code	

config syslog host

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

informational – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above.

warning – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above.

all – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host.

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.

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

config syslog host

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.

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

Restrictions

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

Example usage:

To configure a Syslog host:

```
DES-3528:5#config syslog host 1 severity all
Command: config syslog host 1 severity all
Success.

DES-3528:5#
```

Example usage:

To configure a syslog host for all hosts:

```
DES-3528:5#config syslog host all severity all
Command: config syslog host all severity all
Success.

DES-3528:5#
```

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	<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>all – Specifies that the command will be applied to all hosts.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DES-3528:5#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3528:5#
```

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-3528:5#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-3528:5#
```

config log_save_timing

Purpose	Used to configure the method to save log.
Syntax	config log_save_timing [time_interval <min 1-65535> on_demand log_trigger]
Description	This command is used to set the method to save log.
Parameters	<p><i>time_interval</i> – save log to flash every xxx minutes. (if no log happen in this period, don't save)</p> <p><i>on_demand</i> – save log to flash whenever user type "save log" or "save all" This is also the default.</p> <p><i>log_trigger</i> – save log to flash whenever log arrives</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure log_save_timing:

```
DES-3528:5# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DES-3528:5#
```

show log_save_timing

Purpose	Used to show the timing method to save log.
Syntax	show log_save_timing
Description	This command is used to show method to save log.
Parameters	None.
Restrictions	None.

Example usage:

To show log_save_timing:

```
DES-3528:5# show log_save_timing
Command: show log_save_timing

Saving Log Method: On_demand

DES-3528:5#
```

show attack_log

Purpose	Used to show dangerous log messages.
Syntax	show attack_log {unit <unit_id 1-8>} {index <value_list>}
Description	This command is used to show content of dangerous log messages.
Parameters	<p><i>unit</i> – Specifies the unit of which the attack_log will be show. if it is not specified, it refers to the master unit.</p> <p><i>value_list X-Y</i> – The show log command will display the dangerous log messages between the log number of X and Y. For example, show dangerous log index 1-5 will display the dangerous log messages from 1 to 5.</p> <p>If no parameter specified, all dangerous log entries will be displayed.</p>
Restrictions	None.

Example usage:

To show dangerous messages on master:

```
DES-3528:5#show attack_log
Command: show attack_log

Index   Time                Log Text
-----  -
2       00000 days 01:25:43  Possible spoofing attack from 000d01002301 port 6:3
1       00000 days 01:25:43  Possible spoofing attack from 000d01002301 port 6:3

DES-3528:5#
```

clear attack_log

Purpose	Used to clear the Switch's dangerous log.
Syntax	clear attack_log {unit <unit_id 1-8>}
Description	This command clears the Switch's dangerous log.
Parameters	<i>unit</i> - Specifies the unit of which the attack_log will be cleared. if it is not specified, it refers to the master unit.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the master's dangerous log:

```
DES-3528:5#clear attack_log
Command: clear attack_log

Success.

DES-3528:5#
```

config system_severity

Purpose	Used to configure system_severity level of an alert required for log entry or trap message.
Syntax	config system_severity [trap log all] [critical warning information]
Description	<p>This command is used to configure the system_severity levels on the Switch. When an event occurs on the Switch, a message will be sent to the SNMP agent (trap), the Switch's log or both. Events occurring on the Switch are separated into three main categories, these categories are NOT precisely the same as the parameters of the same name (see below).</p> <ul style="list-style-type: none"> • Information – Events classified as information are basic events occurring on the Switch that are not deemed as problematic, such as enabling or disabling various functions on the Switch. • Warning – Events classified as warning are problematic events that are not critical to the overall function of the Switch but do require attention, such as unsuccessful downloads or uploads and failed logins. • Critical – Events classified as critical are fatal exceptions occurring on the Switch, such as hardware failures or spoofing attacks.
Parameters	<p>Choose one of the following to identify where severity messages are to be sent.</p> <ul style="list-style-type: none"> • <i>trap</i> – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent for analysis. • <i>log</i> – Entering this parameter will define which events occurring on the Switch will be sent to the Switch's log for analysis. • <i>all</i> – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent and the Switch's log for analysis. <p>Choose one of the following to identify what level of severity warnings are to be sent to the destination entered above.</p> <p><i>critical</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send only critical events to the Switch's log or SNMP agent.</p> <p><i>warning</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send critical and warning events to the Switch's log or SNMP agent.</p> <p><i>information</i> – Entering this parameter along with the proper destination, stated above, will instruct the switch to send informational, warning and critical events to the Switch's log or SNMP agent.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the system severity settings:

```
DES-3528:5#config system_severity trap critical
Command: config system_severity trap critical
```

Success.

```
DES-3528:5#
```

show system_severity

Purpose	Used to display system_severity level of an alert required for log entry or trap message.
Syntax	show system_severity
Description	This command is used to display system_severity level of an alert required for log entry or trap message.
Parameters	None.
Restrictions	None.

Example usage:

To display the system severity settings for critical traps and log:

```
DES-3528:5#show system_severity
Command: show system_severity

System Severity Trap : information
System Severity Log : information

DES-3528:5#
```

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 4096 element table (defined here as a *vid_range*) which will associate each of the possible 4096 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.

Command	Parameters
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] nni_bpdu_addr [dot1d dot1ad]}(1)
config stp ports	<portlist> { externalCost [auto <value 1-200000000>] hellotime <value 1-2> migrate [yes no] edge [true false auto] p2p [true false auto] state [enable disable] restricted_role [true false] restricted_tcn [true false] fbpdudisable [enable disable] }(1)
create stp instance_id	<value 1-15>
config stp instance_id	<value 1-15> [add_vlan remove_vlan] <vidlist>
delete stp instance_id	<value 1-15>
config stp priority	<value 0-61440> instance_id <value 0-15>
config stp mst_config_id	{revision_level <int 0-65535> name <string>}(1)
config stp mst_ports	<portlist> instance_id <value 0-15> {internalCost [auto <value 1-200000000>] priority <value 0-240>}(1)
show stp	
show stp ports	{<portlist>}

Command	Parameters
show stp instance	{<value 0-15>}
config stp nni_bpdu_addr	[dot1d dot1ad]
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 allows the Spanning Tree Protocol to be globally enabled on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DES-3528:5#enable stp
Command: enable stp

Success.

DES-3528:5#
```

disable stp

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

Example usage:

To disable STP on the Switch:

```
DES-3528:5#disable stp
Command: disable stp

Success.

DES-3528:5#
```

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 allows the user to choose the version of the spanning tree to be implemented on the Switch.
Parameters	<i>mstp</i> – Selecting this parameter will set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. <i>rstp</i> – Selecting this parameter will set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. <i>stp</i> – Selecting this parameter will set the Spanning Tree Protocol (STP) globally on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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


```
DES-3528:5#config stp version mstp
```

```
Command: config stp version mstp
```

```
Success
```

```
DES-3528:5#
```

config stp

Purpose	Used to setup STP, RSTP and MSTP on the Switch.
Syntax	config stp {maxage <value 6-40> maxhops <value 6-40> hellotime <value 1-2> forwarddelay <value 4-30> txholdcount <value 1-10> fbpdu [enable disable] nni_bpdu_addr [dot1d dot1ad]}(1)
Description	This command is used to setup 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><i>maxage <value 6-40></i> – 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><i>maxhops <value 6-40></i> – 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><i>hellotime <value 1-2></i> – 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> <div style="display: flex; align-items: center;">  <p>NOTE: In MSTP, the spanning tree is configured by port and therefore, the <i>hellotime</i> must be set using the <i>configure stp ports</i> command for switches utilizing the Multiple Spanning Tree Protocol.</p> </div> <p><i>forwarddelay <value 4-30></i> – 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><i>txholdcount <value 1-10></i> – The maximum number of BPDU Hello packets transmitted per interval. Default value is 6.</p> <p><i>fbpdu [enable disable]</i> – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is <i>enable</i>.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DES-3528:5#config stp maxage 18 maxhops 15
```

```
Command: config stp maxage 18 maxhops 15
```

```
Success.
```

```
DES-3528:5#
```


config stp ports

Purpose	Used to setup 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] p2p [true false auto] state [enable disable] restricted_role [true false] restricted_tcn [true false] fbpdu [enable disable] }(1)
Description	This command is used to create and configure STP for a group of ports.
Parameters	<p><i><portlist></i> – Specifies a range of ports to be configured.</p> <p><i>externalCost</i> – 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 <i>auto</i>.</p> <p><i>auto</i> – 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><i><value 1-200000000></i> – 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><i>hellotime <value 1-2></i> – 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><i>migrate [yes no]</i> – 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 <i>yes</i> 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><i>edge [true false auto]</i> – <i>true</i> 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. <i>false</i> indicates that the port does not have edge port status.</p> <p><i>auto</i> – Indicates that the port will be able to automatically enable the edge port status if this port links to an end station or a device that does not support the STP function.</p> <p><i>restricted_role [true false]</i> – If <i>true</i> causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be <i>false</i> by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.</p> <p><i>restricted_tcn [true false]</i> – If <i>true</i> causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter should be <i>false</i> by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or MAC_Operational for the attached LANs transitions frequently.</p> <p><i>p2p [true false auto]</i> – <i>true</i> 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 <i>p2p</i> value of <i>false</i> indicates that the port cannot have <i>p2p</i> status. <i>Auto</i> allows the port to have <i>p2p</i> status whenever possible and operate as if the <i>p2p</i> status were <i>true</i>. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the <i>p2p</i> status changes to operate as if the <i>p2p</i> value were <i>false</i>. The default setting for this</p>

config stp ports

parameter is *auto*.

state [enable | disable] – Allows STP to be enabled or disabled for the ports specified in the port list. The default is *enable*.

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

Example usage:

To configure STP with path cost 19, hellotime set to 2 seconds, migration enabled, and state enabled for ports 1-5 of module 1.

```
DES-3528:5#config stp ports 1-5 externalCost 19 hellotime 2 migrate yes state enable
Command: config stp ports 1-5 externalCost 19 hellotime 2 migrate yes state enable

Success.

DES-3528:5#
```

create stp instance_id

Purpose Used to create a STP instance ID for MSTP.

Syntax **create stp instance_id <value 1-15>**

Description This command allows the user to create a STP instance ID for the Multiple Spanning Tree Protocol. There are 16 STP instances on the Switch (one internal CIST, unchangeable) and the user may create up to 15 instance IDs for the Switch.

Parameters *<value 1-15>* – Enter a value between 1 and 15 to identify the Spanning Tree instance on the Switch.

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

Example usage:


To create a spanning tree instance 2:

```
DES-3528:5#create stp instance_id 2
Command: create stp instance_id 2

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

DES-3528:5#
```

config stp instance_id

Purpose	Used to add or delete VID to/from an STP instance.
Syntax	config stp instance_id <value 1-15> [add_vlan remove_vlan] <vidlist>
Description	This command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an <i>instance_id</i> . 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 16 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time.  NOTE: Switches in the same spanning tree region having the same STP <i>instance_id</i> must be mapped identically, and have the same configuration <i>revision_level</i> number and the same <i>name</i> .
Parameters	<i><value 1-15></i> – Enter a number between 1 and 15 to define the <i>instance_id</i> . The Switch supports 16 STP instances with one unchangeable default instance ID set as 0. <i>add_vlan</i> – Along with the <i>vid_range <vidlist></i> parameter, this command will add VIDs to the previously configured STP <i>instance_id</i> . <i>remove_vlan</i> – Along with the <i>vid_range <vidlist></i> parameter, this command will remove VIDs to the previously configured STP <i>instance_id</i> . <i><vidlist></i> – Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DES-3528:5#config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.

DES-3528:5#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DES-3528:5#config stp instance_id 2 remove_vlan 10
Command : config stp instance_id 2 remove_vlan 10

Success.

DES-3528:5#
```

delete stp instance_id

Purpose	Used to delete a STP instance ID from the Switch.
Syntax	delete stp instance_id <value 1-15>
Description	This command allows the user to delete a previously configured STP instance ID from the Switch.
Parameters	<i><value 1-15></i> – Enter a value between 1 and 15 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete STP instance ID 2 from the Switch.

```
DES-3528:5#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DES-3528:5#
```

config stp priority

Purpose	Used to configure the bridge priority.
Syntax	config stp priority <value 0-61440> instance_id <value 0-15>
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 <i>instance_id</i> for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	<p><i>priority <value 0-61440></i> – 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 value must be divisible by 4096.</p> <p><i>instance_id <value 0-15></i> – 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 <i>instance_id</i> (CIST) internally set on the Switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the priority value for *instance_id 2* as 4096.

```
DES-3528:5#config stp priority 4096 instance_id 2
Command : config stp priority 4096 instance_id 2

Success.

DES-3528:5#
```

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 32>}(1)
Description	This command will 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 <i>revision_level</i> and <i>name</i> will be considered as part of the same MSTP region.
Parameters	<p><i>revision_level <int 0-65535></i>– 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><i>name <string></i> – Enter an alphanumeric string of up to 32 characters to uniquely identify the MSTP region on the Switch. This <i>name</i>, along with the <i>revision_level</i> value will identify the MSTP region configured on the Switch. If no <i>name</i> is entered, the default name will be the MAC address of the device.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MSTP region of the Switch with *revision_level 10* and the *name* “Trinity”:

```
DES-3528:5#config stp mst_config_id revision_level 10 name Trinity
Command : config stp mst_config_id revision_level 10 name Trinity

Success.

DES-3528:5#
```

config stp mst_ports

Purpose	Used to update the port configuration for a MSTP instance.
Syntax	config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto <value 1-200000000>] priority <value 0-240>}(1)
Description	This command will update the port configuration for a STP <i>instance_id</i> . 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><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p><i>instance_id <value 0-15></i> – Enter a numerical value between 0 and 15 to identify the <i>instance_id</i> previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree).</p> <p><i>internalCost</i> – 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 <i>auto</i>. There are two options:</p> <ul style="list-style-type: none"> <i>auto</i> – Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. <i>value 1-200000000</i> – Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower <i>internalCost</i> represents a quicker transmission. <p><i>priority <value 0-240></i> – 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. This value must be divisible by 16.</p>
Restrictions	Only Administrator and Operator-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-3528:5#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-3528:5#
```

show stp

Purpose	Used to display the Switch's current STP configuration.
Syntax	show stp
Description	This command displays 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-3528:5#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      : 3
Forwarding BPDU    : Enabled
NNI BPDU Address   : dot1ad

DES-3528:5#
```

Status 2 : STP enabled for RSTP

```
DES-3528:5#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      : 3
Forwarding BPDU    : Enabled
NNI BPDU Address   : dot1ad

DES-3528:5#
```

Status 3 : STP enabled for MSTP

```
DES-3528:5#show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status          : Enabled
STP Version         : MSTP
Max Age            : 20
Forward Delay      : 15
Max Hops           : 20
TX Hold Count      : 3
Forwarding BPDU    : Enabled
NNI BPDU Address   : dot1ad

DES-3528:5#
```

show stp ports

Purpose	Used to display the Switch's current STP ports configuration.
Syntax	show stp ports <portlist>
Description	This command displays the STP ports settings for a specified port or group of ports (one port at a time).
Parameters	<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.
Restrictions	None.

Example usage:

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

```
DES-3528:5#show stp ports
Command: show stp ports

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

show stp instance

Purpose	Used to display the Switch's STP instance configuration
Syntax	show stp instance <value 0-15>
Description	This command displays the Switch's current STP Instance Settings and the STP Instance Operational Status.
Parameters	<value 0-15> – Enter a value defining the previously configured <i>instance_id</i> 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-3528:5#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
```

config stp nni_bpdu_addr

Purpose	Used to configure BPDU destination address as dot1d or dot1ad.
Syntax	config stp nni_bpdu_addr [dot1d dot1ad]
Description	This command is to configure the NNI-port-sent BPDU destination address to 802.1ad address (0180c200000D) or 802.1d address (0180c2000021). When the Q-in-Q is enabled., NNI-port-sent BPDU destination address will set to dot1ad. The user can configure the NNI port send BPDU destination address to dot1d. The default is <i>dot1d</i> .
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the STP BPDU destination address as dot1 ad on the Switch:

```
DES-3528:5#config stp nni_bpdu_addr dot1ad
Command: config stp nni_bpdu_addr dot1ad

Success.

DES-3528:5#
```

show stp mst_config_id

Purpose	Used to display the MSTP configuration identification.
Syntax	show stp mst_config_id
Description	This command displays 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-3528:5#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         2-4094
1           1

DES-3528:5#
```

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> vlanid <vidlist>] <macaddr> port <port>
create fdb	[<vlan_name 32> vlanid <vidlist>] <macaddr> drop
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add delete] <portlist>
config fdb aging_time	<sec 10-1000000>
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 drop aging_time}
config multicast_vlan_filtering_mode	[vlanid <vidlist> vlan <vlan_name 32> all] [forward_all_groups forward_unregistered_groups filter_unregistered_groups]
show multicast_vlan_filtering_mode	{[vlanid <vidlist> vlan <vlan_name 32>]}

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

create fdb

Purpose	Used to create a static entry to the unicast MAC address forwarding table (database).
Syntax	create fdb [<vlan_name 32> vlanid <vidlist>] <macaddr> port <port>
Description	This command will make an entry into 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>vlanid <vidlist> - The list of VLANs by VLAN ID.</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 and Operator-level users can issue this command.

Example usage:

To create a unicast MAC FDB entry:

```
DES-3528:5#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-3528:5#
```

create fdb drop

Purpose	Used to create a static entry to filter the packet with specified MAC address based on either source or destination MAC addresses.
Syntax	create fdb [<vlan_name32> vlanid <vidlist>] <macaddr> drop
Description	This command is used to create a static entry to filter the packet with specified MAC address based on either source or destination MAC addresses.
Parameters	<p><vlan_name > – The name of the VLAN on which the MAC address resides.</p> <p><vlanid_list> – Specifies a range of VLANs to be configured.</p> <p><macaddr> – The MAC address that will be added to the forwarding table.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To filter an unicast MAC:

```
DES-3528:5#create fdb default 00-00-00-33-01-02 drop
Command: create fdb default 00-00-00-33-01-02 drop

Success.

DES-3528:5#
```

create multicast_fdb

Purpose	Used to create a static entry to the multicast MAC address forwarding table (database)
Syntax	create multicast_fdb <vlan_name 32> <macaddr>
Description	This command will make an entry into 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 and Operator-level users can issue this command.

Example usage:

To create multicast MAC forwarding:

```
DES-3528:5#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DES-3528:5#
```

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 configures 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 and Operator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DES-3528:5#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-3528:5#
```

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 and Operator-level users can issue this command.

Example usage:

To set the FDB aging time:

```
DES-3528:5#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3528:5#
```

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	<i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides. <i><macaddr></i> – The MAC address that will be added to the forwarding table.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DES-3528:5#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3528:5#
```

To delete a multicast FDB entry:

```
DES-3528:5#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DES-3528:5#
```

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	<i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides. <i>port <port></i> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. <i>all</i> – Clears all dynamic entries to the Switch's forwarding database.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

```
DES-3528:5#clear fdb all
Command: clear fdb all

Success.

DES-3528:5#
```

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	<vlan_name 32> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that is present in the forwarding database table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DES-3528:5#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-3528:5#
```

show fdb

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	show fdb { port <port> [vlan <vlan_name 32> vlanid <vidlist>] mac_address <macaddr> static drop aging_time}
Description	This command will display the current contents of the Switch's forwarding database.
Parameters	<i>port</i> <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. <i>vlanid</i> <vidlist> - The list of VLANs by VLAN ID. <macaddr> – The MAC address that is present in the forwarding database table. <i>static</i> – Displays the static MAC address entries. <i>drop</i> - Displays the drop MAC address entries. <i>aging_time</i> – Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DES-3528:5#show fdb
```

```
Command: show fdb
```

```
Unicast MAC Address Aging Time = 300
```

VID	VLAN Name	MAC Address	Port	Type
1	default	00-00-5E-00-01-5F	15	Dynamic
1	default	00-00-81-00-00-01	15	Dynamic
1	default	00-00-81-9A-F2-F4	15	Dynamic
1	default	00-00-E2-2F-44-EC	15	Dynamic
1	default	00-01-23-55-1A-28	15	Dynamic
1	default	00-01-6C-CE-62-E0	15	Dynamic
1	default	00-02-A5-FD-66-97	15	Dynamic
1	default	00-03-09-18-10-01	15	Dynamic
1	default	00-03-9D-73-32-F0	15	Dynamic
1	default	00-03-B3-00-09-E9	15	Dynamic
1	default	00-04-00-00-00-00	15	Dynamic
1	default	00-05-5D-04-D6-A4	15	Dynamic
1	default	00-05-5D-25-45-61	15	Dynamic
1	default	00-05-5D-6A-A5-2C	15	Dynamic
1	default	00-05-5D-9A-FE-6D	15	Dynamic
1	default	00-05-5D-DB-BA-7C	15	Dynamic
1	default	00-05-5D-ED-84-52	15	Dynamic
1	default	00-05-5D-ED-84-7B	15	Dynamic

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

config multicast vlan_filtering_mode

Purpose	Used to configure the the multicast packet filtering mode for VLANs.
Syntax	config multicast vlan_filtering_mode [vlanid <vidlist> vlan <vlan_name 32> all] [forward_all_groups forward_unregistered_groups filter_unregistered_groups]
Description	The command configures the multicast packet filtering mode for VLANs.
Parameters	<p><i>vlanid_list</i> – Specifies a range of VLANs to be configured.</p> <p>The filtering mode can be any of the following:</p> <p><i>forward_all_groups</i> - All multicast groups will be forwarded based on VLAN.</p> <p><i>forward_unregistered_groups</i> - The registered group will be forwarded based on the register table.The unregister group will be forwarded based on VLAN.</p> <p><i>filter_unregistered_groups</i> - The registered group will be forwarded based on the register table.The unregister group will be filtered.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the multicast packet filtering mode for vlans:

```
DES-3528:5# config multicast vlan_filtering_mode vlan 200-300 forward_all_groups
```

```
Command: config multicast vlan_filtering_mode vlan 200-300 forward_all_groups
```

```
Success.
```

```
DES-3528:5#
```

show multicast vlan_filtering_mode

Purpose	Used to show the multicast packet filtering mode for VLANs.
Syntax	show multicast vlan_filtering_mode {[vlanid <vidlist> vlan <vlan_name 32>]}
Description	The command displays the multicast packet filtering mode for VLAN.
Parameters	<i>vlanid_list</i> – Specifies a range of vlans to be configured. If no parameter specified , the device will show all multicast filtering settings in the device.
Restrictions	None.

Example usage:

To display multicast VLAN filtering mode for VLANs:

```
DES-3528:5# show multicast vlan_filtering_mode
Command: show multicast vlan_filtering_mode

VLAN ID/VLAN Name          Multicase Filter Mode
-----
100 /Sales                 forward_all_groups
200 /PM                    forward_all_groups
600 /Customer              filter unregistered groups

Total Entries : 3

DES-3528:5#
```


TRAFFIC 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 do 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 window 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 the packet storm discontinues before the countdown timer expires, the port will again allow all incoming traffic. If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the port will be recovered after 5 minutes, or the user manually resets the port using the **config ports enable** command, mentioned previously in this manual.

The broadcast 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 0-255000> time_interval <value 5-30> countdown [<value 0> <value 5-30>]}(1)
show traffic control	{[<portlist>]}
config traffic 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	config traffic control [<portlist> all] { broadcast [enable disable] multicast [enable disable] unicast [enable disable] action [drop shutdown] threshold <value 0-255000> time_interval <value 5-30> countdown [<value 0> <value 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 group list of ports to be configured for traffic control, as defined below:</p> <ul style="list-style-type: none"> <i>all</i> – Specifies all portlists are to be configured for traffic control on the Switch. <i>broadcast</i> [enable disable] – Enables or disables broadcast storm control. <i>multicast</i> [enable disable] – Enables or disables multicast storm control. <i>unicast</i> [enable disable] – Enables or disables unicast traffic control. <p><i>action</i> – 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"> • <i>drop</i> – 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. • <i>shutdown</i> – Utilizes the Switch's software Traffic Control mechanism to determine

config traffic control

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 Shutdown Forever mode. It can be recovered after 5 minutes, or the user manually resets the port using the **config ports 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.

threshold <value 0-255000> – The upper threshold at which the specified traffic control is switched on. The *<value>* is the number of broadcast/multicast/unicast packets, in packets per second (pps), received by the Switch that will trigger the storm traffic control measures. The default setting is 131072.

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.

value 5-30 – The Interval may be set between 5 and 30 seconds with the default setting of 5 seconds.

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. The Switch will shutdown the port only if the traffic level exceeds the previously configured threshold all the time during this countdown period. 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.

- *value 0* – 0 is the default setting for this field and 0 will denote that the port will never shutdown.
- *value 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 shutdown forever mode and can only be manually recovered using the config ports command mentioned previously in this manual.

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

Example usage:

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

```
DES-3528:5#config traffic control 1-12 broadcast enable action shutdown threshold 1
countdown 10 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown threshold 1
countdown 10 time_interval 10
Success.
DES-3528:5#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	show traffic control { <portlist> }
Description	This command displays the current storm traffic control configuration on the Switch.
Parameters	<i><portlist></i> – 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 settings:

```
DES-3528:5#show traffic control
```

```
Command: show traffic control
```

```
Traffic Storm Control Trap :[None]
```

Port	Thres hold	Broadcast Storm	Multicast Storm	Unicast Storm	Action	Count Down	Time Interval
1	131072	Disabled	Disabled	Disabled	drop	0	5
2	131072	Disabled	Disabled	Disabled	drop	0	5
3	131072	Disabled	Disabled	Disabled	drop	0	5
4	131072	Disabled	Disabled	Disabled	drop	0	5
5	131072	Disabled	Disabled	Disabled	drop	0	5
6	131072	Disabled	Disabled	Disabled	drop	0	5
7	131072	Disabled	Disabled	Disabled	drop	0	5
8	131072	Disabled	Disabled	Disabled	drop	0	5
9	131072	Disabled	Disabled	Disabled	drop	0	5
10	131072	Disabled	Disabled	Disabled	drop	0	5
11	131072	Disabled	Disabled	Disabled	drop	0	5
12	131072	Disabled	Disabled	Disabled	drop	0	5
13	131072	Disabled	Disabled	Disabled	drop	0	5
14	131072	Disabled	Disabled	Disabled	drop	0	5
15	131072	Disabled	Disabled	Disabled	drop	0	5
16	131072	Disabled	Disabled	Disabled	drop	0	5

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

config traffic trap

Purpose	Used to configure the trap settings for the packet storm control mechanism.
Syntax	config traffic trap [none storm_occurred storm_cleared both]
Description	This command is used to configure how packet storm control trap messages will be used when a packet storm is detected by the Switch. This function can only be used for the software traffic storm control mechanism (when the action field in the config traffic storm_control command is set as shutdown).
Parameters	<p><i>none</i> – No notification will be generated or sent when a packet storm control is detected by the Switch.</p> <p><i>storm_occurred</i> – A notification will be generated and sent when a packet storm has been detected by the Switch.</p> <p><i>storm_cleared</i> – A notification will be generated and sent when a packet storm has been cleared by the Switch.</p> <p><i>both</i> – A notification will be generated and sent when a packet storm has been detected and cleared by the Switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure notifications to be sent when a packet storm control has been detected and cleared by the Switch.

```
DES-3528:5#config traffic trap both
```

```
Command: config traffic trap both
```

```
Success.
```

```
DES-3528:5#
```

QoS COMMANDS

The Switch supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 6 (Class 6) — 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 Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q6 queue.
- Q7 is reserved for stacking function.

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the eight hardware priority queues in order, beginning with the highest priority queue, 6, 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 commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config bandwidth_control	[<portlist> all] {rx_rate [no_limit <value 64-1024000>] tx_rate [no_limit <value 64-1024000>]}(1)
show bandwidth_control	{<portlist>}
config cos bandwidth_control	{ports [<portlist> all]} <cos_id_list 0-6> {min_rate [no_limit <value 64-1024000>] max_rate [no_limit <value 64-1024000>]}(1)
show cos bandwidth_control	{<portlist>}
config scheduling	{ports [<portlist> all]} <class_id 0-6> [strict weight <value 1-127>]
config scheduling_mechanism	{ports [<portlist> all]} [strict wrr]
show scheduling	{<portlist>}
show scheduling_mechanism	{<portlist>}
config 802.1p user_priority	{ports [<portlist> all]} <priority 0-7> <class_id 0-6>
show 802.1p user_priority	{<portlist>}
config 802.1p default_priority	[<portlist> all] <priority 0-7>
show 802.1p default_priority	<portlist>
enable hol_prevention	
disable hol_prevention	
show hol_prevention	

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> all] {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 (<i>no_limit</i> or <value 64-1024000>) will be applied to the rate at which the above specified ports will be allowed to receive packets</p> <ul style="list-style-type: none"> ▪ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ <value 64-1024000> – Specifies the packet limit, in Kbps, that the above ports will be allowed to receive. <p>tx_rate – Specifies that one of the parameters below (<i>no_limit</i> or <value 64-1024000>) will be applied to the rate at which the above specified ports will be allowed to transmit packets.</p> <ul style="list-style-type: none"> ▪ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ <value 64-1024000> – Specifies the packet limit, in Kbps, that the above ports will be allowed to receive.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DES-3528:5#config bandwidth_control 1-10 tx_rate 64
Command: config bandwidth_control 1-10 tx_rate 64

Success.

DES-3528:5#
```

show bandwidth_control

Purpose	Used to display the bandwidth control table.
Syntax	show bandwidth_control {<portlist>}
Description	This command displays 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 port bandwidth control table:

```
DES-3528:5#show bandwidth_control 1-10
```

```
Command: show bandwidth_control 1-10
```

Bandwidth Control Table

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1	No Limit	No Limit	No Limit	No Limit
2	No Limit	No Limit	No Limit	No Limit
3	No Limit	No Limit	No Limit	No Limit
4	No Limit	No Limit	No Limit	No Limit
5	No Limit	No Limit	No Limit	No Limit
6	No Limit	No Limit	No Limit	No Limit
7	No Limit	No Limit	No Limit	No Limit
8	No Limit	No Limit	No Limit	No Limit
9	No Limit	No Limit	No Limit	No Limit
10	No Limit	No Limit	No Limit	No Limit

```
DES-3528:5#
```

config cos bandwidth_control

Purpose Used to configure per port or flow bandwidth control. For per flow bandwidth control, it can be based on the assigned CoS queue.

Syntax `config cos bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-6> {min_rate [no_limit | <value 64-1024000>] max_rate [no_limit | <value 64-1024000>]}(1)`

Description This command is used to set per port or flow bandwidth control. For per flow bandwidth control, it can be based on the assigned CoS queue.

Mini-rate specifies the minimal guaranteed bandwidth. Specify no limit for the mini-rate means no guaranteed bandwidth.

Max-rate specifies the max-rate limitation. When it is specified, packet transmitted from the queue will not exceed the specified max-rate limitation even though there is still available bandwidth.

The specification of mini-rate and max-rate are effective regardless whether the queue is operated in the strict mode or in the wrr mode.

Parameters *<portlist>* – Specifies a port or range of ports to be configured.

<cos_id_list 0-6> – Specifies a priority queue.

min_rate - Specifies one of the parameters below (*no_limit* or *<value 64-1024000>*) that will be applied to the minimum rate at which the above specified class will be allowed to receive packets.

- *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified class.
- *<value 64-1024000>* – Specifies the packet limit, in Kbps, that the above ports will be receive at least.

max_rate – Specifies one of the parameters below (*no_limit* or *<value 64-1024000>*) that will be applied to the maximum rate at which the above specified class will be allowed to receive packets.

- *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified class.
- *<value 64-1024000>* – Specifies the packet limit, in Kbps, that the above ports will be received at most.

config cos bandwidth_control

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

Example usage:

To configure CoS bandwidth control:

```
DES-3528:5#config cos bandwidth_control ports 1-10 2 min_rate 100 max_rate 200
Command: config cos bandwidth_control ports 1-10 2 min_rate 100 max_rate 200

The setting values are not a multiple of 64, closest values 128 and 192 are chosen.

Success.

DES-3528:5#
```

show cos bandwidth_control

Purpose Used to display the per port per cos queue bandwidth control setting.

Syntax **show cos bandwidth_control {<portlist>}**

Description This command is used to display the per port per cos queue bandwidth control setting.

Parameters <portlist> – Specifies a port or range of ports to be viewed.

Restrictions None.

Example usage:

To display port per cos bandwidth control table:

```
DES-3528:5#show cos bandwidth_control 10
Command: show cos bandwidth_control 10

Class Bandwidth Control Table On Port: 10

Class      Min Rate(Kbit/sec)      Max Rate(Kbit/sec)
0          No Limit                No Limit
1          No Limit                No Limit
2          No Limit                No Limit
3          No Limit                No Limit
4          No Limit                No Limit
5          No Limit                No Limit
6          No Limit                No Limit

DES-3528:5#
```


config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	config scheduling {ports [<portlist> all]} <class_id 0-6> [strict weight <value 1-127>]
Description	<p>The Switch contains eight hardware priority queues. Incoming packets must be mapped to one of these eight queues. This command is used to specify the rotation mechanism regarding how packets in these eight hardware priority queues are being handled and emptied.</p> <p>The Switch's default (if the config scheduling command is not used, or if the config scheduling command is entered with <i>weight</i> parameters set to 0) is to empty the 7 hardware priority queues in order – from the highest priority queue (hardware queue 6) 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>The <i>weight</i> parameter allows the user to specify the maximum number of packets a given hardware priority queue can transmit before allowing the next lower hardware priority queue to begin transmitting its packets. A value between 0 and 127 can be specified. For example, if a value of 3 is specified, then the highest hardware priority queue (number 6) will be allowed to transmit 3 packets – then the next lower hardware priority queue (number 5) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat.</p>
Parameters	<p><i><class_id 0-6></i> – Specifies which of the seven hardware priority queues that the config scheduling command will apply to. The seven hardware priority queues are identified by number, from 0 to 6, with the queue 0 being the lowest priority.</p> <p><i>[<portlist> all]</i> – Specifies a range of ports to be configured.</p> <p><i>strict</i> – Specifies this queue is always working in strict mode.</p> <p><i>weight <value 1-127></i> – Using weighted fair algorithm to handle packets in priority queues. Each queue will operate based on its setting of weight values.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the traffic scheduling for each CoSqueue:

```
DES-3528:5# config scheduling ports 10 3 strict
```

```
Command: config scheduling ports 10 3 strict
```

```
Success.
```

```
DES-3528:5#
```

config scheduling mechanism

Purpose	Used to configure the traffic scheduling mechanism for a port or a range of ports.
Syntax	config scheduling_mechanism {ports [<portlist> all]} [strict wrr]
Description	This command is used to specify how the switch handles packets in priority queues.
Parameters	<p><i><portlist></i> – Select a port or a list of ports to configure.</p> <p><i>all</i> – Choose this option to select all ports.</p> <p><i>strict</i> – The highest queue first process. That is, the highest queue should always be processed first.</p> <p><i>wrr</i> – Using weighted roundrobin algorithm to handle packets in priority queues.</p>

config scheduling mechanism

Restrictions Only Administrator and Operation-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DES-3528:5#config scheduling_mechanism ports 1 strict
Command: config scheduling_mechanism ports 1 strict

Success.

DES-3528:5#
```

show scheduling

Purpose	Used to display the current configured traffic scheduling for a port or a range of ports on the Switch.
Syntax	show scheduling {<portlist>}
Description	This command will display the current traffic scheduling settings for a port or a range of ports on the Switch.
Parameters	<portlist> – Specifies a port or a range of ports to be displayed.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```

DES-3528:5#show scheduling
Command: show scheduling

QOS Output Scheduling On Port: 1:1

Class ID  Weight
-----  -
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7

QOS Output Scheduling On Port: 1:2

Class ID  Weight
-----  -
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7

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

```

show scheduling_mechanism

Purpose	Used to show the current traffic scheduling mechanism for a port or a range of ports on the Switch.
Syntax	show scheduling_mechanism {<portlist>}
Description	This command is used to display the current traffic scheduling mechanism for a port or a range of ports on the Switch.
Parameters	<portlist> – Specifies a range of ports to be displayed.
Restrictions	None.

Example usage:

To display the scheduling mechanism:

```
DES-3528:5#show scheduling_mechanism 1-4
```

```
Command: show scheduling_mechanism 1-4
```

```
Port    Mode
-----  -----
1       Strict
2       Strict
3       Strict
4       Strict
```

```
DES-3528:5#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues on the Switch.																											
Syntax	config 802.1p user_priority {ports [<portlist> all]} <priority 0-7> <class_id 0-6>																											
Description	<p>This command allows users to configure the way the Switch will map an incoming packet, based on its 802.1p user priority, to one of the eight available hardware priority queues on the Switch.</p> <p>The Switch's default is to map the following incoming 802.1p user priority values to the eight 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>2</td> <td>Mid-low</td> </tr> <tr> <td>1</td> <td>0</td> <td>Lowest</td> </tr> <tr> <td>2</td> <td>1</td> <td>Lowest</td> </tr> <tr> <td>3</td> <td>3</td> <td>Mid-low</td> </tr> <tr> <td>4</td> <td>4</td> <td>Mid-high</td> </tr> <tr> <td>5</td> <td>5</td> <td>Mid-high</td> </tr> <tr> <td>6</td> <td>6</td> <td>Highest</td> </tr> <tr> <td>7</td> <td>6</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 0-6> (the number of the hardware queue).</p>	802.1p	Hardware Queue	Remark	0	2	Mid-low	1	0	Lowest	2	1	Lowest	3	3	Mid-low	4	4	Mid-high	5	5	Mid-high	6	6	Highest	7	6	Highest.
802.1p	Hardware Queue	Remark																										
0	2	Mid-low																										
1	0	Lowest																										
2	1	Lowest																										
3	3	Mid-low																										
4	4	Mid-high																										
5	5	Mid-high																										
6	6	Highest																										
7	6	Highest.																										
Parameters	<p>[<portlist> all] – Specifies a range of ports to be configured. All specifies all ports.</p> <p><priority 0-7> – The 802.1p user priority to associate with the <class_id 0-6> (the number of the hardware queue).</p> <p><class_id 0-6> – The number of the Switch's hardware priority queue. The Switch has seven hardware priority queues available. They are numbered between 0 (the lowest priority) and 6 (the highest priority).</p>																											
Restrictions	Only Administrator and Operator-level users can issue this command.																											

Example usage:

To configure 802.1p user priority on the Switch:

```
DES-3528:5#config 802.1p user_priority ports 1 5 5
```

```
Command: config 802.1p user_priority ports 1 5 5
```

```
Success.
```

```
DES-3528:5#
```

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 eight hardware priority queues.
Syntax	show 802.1p user_priority {<portlist>}
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 seven hardware priority queues.
Parameters	{<portlist>} – Specifies a range of ports to be displayed.
Restrictions	None.

Example usage:

To show 802.1p user priority:

```
DES-3528:5#show 802.1p user_priority 1-2
```

```
Command: show 802.1p user_priority 1-2
```

QOS Class of Traffic

Port 1

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

Port 2

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

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

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 default 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 the default priority for the Switch to handle the untagged packets. The priority value entered with this command will be used to determine which of the seven hardware priority queues the packet is forwarded to.
Parameters	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p>all – Specifies that the command applies to all ports on the Switch.</p> <p><priority 0-7> – The priority value to assign to untagged packets received by the Switch or a range of ports on the Switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the Switch:

```
DES-3528:5#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3528:5#
```

show 802.1 default_priority

Purpose	Used to display the current 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 current 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 configured.
Restrictions	None.

Example usage:

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

```
DES-3528:5#show 802.1p default_priority
Command: show 802.1p default_priority
```

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

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

enable hol_prevention

Purpose	Used to enable the HOL prevention state.
Syntax	enable hol_prevention
Description	This command is used to enable the HOL prevention function on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable HOL prevention:

```
DES-3528:5#enable hol_prevention
Command: enable hol_prevention

Success.
DES-3528:5#
```

disable hol_prevention

Purpose	Used to disable HOL prevention.
Syntax	disable hol_prevention
Description	This command is used to disable the HOL prevention function on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable HOL prevention:

```
DES-3528:5#disable hol_prevention
Command: disable hol_prevention

Success.
DES-3528:5#
```

show hol_prevention

Purpose	Used to show the HOL prevention state.
Syntax	show hol_prevention
Description	This command displays the HOL prevention state.
Parameters	None.
Restrictions	None.

Example usage:

To display HOL prevention:

```
DES-3528:5#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled

DES-3528:5#
```


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><i><port></i> – This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be operating at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.</p> <p><i>[add delete]</i> – Specifies if the user wishes to add or delete ports to be mirrored that are specified in the <i>source ports</i> parameter.</p> <p><i>source ports</i> – The port or ports being mirrored. This cannot include the Target port.</p> <p><i><portlist></i> – 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><i>rx</i> – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p><i>tx</i> – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p><i>both</i> – Mirrors all the packets received or sent by the port or ports in the port list.</p>
Restrictions	<p>The Target port cannot be listed as a source port.</p> <p>Only Administrator and Operator-level users can issue this command.</p>

Example usage:

To add the mirroring ports:

```
DES-3528:5#config mirror port 1 add source ports 2-5 both
```

```
Command: config mirror port 1 add source ports 2-5 both
```

```
Success.
```

```
DES-3528:5#
```

Example usage:

To delete the mirroring ports:

```
DES-3528:5#config mirror port 1 delete source port 2-4 both
Command: config mirror 1 delete source 2-4 both

Success.

DES-3528:5#
```

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 and Operator-level users can issue this command.

Example usage:

To enable mirroring configurations:

```
DES-3528:5#enable mirror
Command: enable mirror

Success.

DES-3528:5#
```

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 and Operator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DES-3528:5#disable mirror
Command: disable mirror

Success.

DES-3528:5#
```

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:

```
Current Settings
Mirror Status: Enabled
Target Port   : 1
Mirrored Port
              RX: 2-5
              TX: 2-5

DES-3528:5#
```

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 2-4094> {type 1q_vlan advertisement}
create vlan vlanid	<vidlist> { advertisement }
delete vlan	<vlan_name 32>
delete vlan vlanid	<vidlist>
config vlan	<vlan_name 32> {[add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable]}(1)
config vlan vlanid	<vidlist> {[add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable] name <vlan_name 32>}(1)
config port_vlan	[<portlist> all] { gvrp_state [enable disable] ingress_checking [enable disable] acceptable_frame[tagged_only admit_all] pvid<vlanid 1-4094> }(1)
enable gvrp	
disable gvrp	
show vlan	{ [<vlan_name 32> vlanid < vidlist > ports {<portlist>}]}
show port_vlan	{<portlist>}
create dot1v_protocol_group	group_id < id 1-16> group_name <name 32>
config dot1v_protocol_group	[group_id <id 1-16> group_name <name 32>][add protocol [ethernet_2 ieee802.3_snap ieee802.3_llc] <protocol_value> delete protocol [ethernet_2 ieee802.3_snap ieee802.3_llc] <protocol_value>]
delete dot1v_protocol_group	[group_id <id 1-16> group_name <name 32> all]
show dot1v_protocol_group	{group_id<id 1-16> group_name <name 32>}
config port dot1v ports	[<portlist> all] [add protocol_group [group_id <id> group_name <name 32>] [vlan< vlan_name 32> vlanid <id>] {priority <value 0-7>} delete protocol_group [group_id <id 1-16> all]]
show port dot1v	{ports <portlist>}
enable pvid auto_assign	
disable pvid auto_assign	
show pvid auto_assign	
config gvrp	[timer [join leave leaveall] < value 100-100000> nni_bpdu_addr [dot1d dot1ad]]
show gvrp	
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.

create vlan

Purpose	Used to create a VLAN on the Switch.
Syntax	create vlan <vlan_name 32 > tag <vlanid 2-4094> { type 1q_vlan advertisement }
Description	This command allows the user to create a VLAN on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN to be created.</p> <p><vlanid 2-4094> – The VLAN ID of the VLAN to be created. Allowed values = 2-4094</p> <p>advertisement – Specifies that the VLAN is able to join GVRP.</p>
Restrictions	Each VLAN name can be up to 32 characters. Up to 4094 static VLANs may be created per configuration. Only Administrator and Operator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DES-3528:5#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DES-3528:5#
```

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 creates multiple VLANs on the switch.
Parameters	<p><vidlist> – Specifies a range of multiple VLAN IDs to be created.</p> <p>advertisement – Join GVRP or not. If not, the VLAN can't join dynamically.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a VLAN ID on the Switch:

```
DES-3528:5#create vlan vlanid 5 advertisement
Command: create vlan vlanid 5 advertisement

Success

DES-3528:5#
```

delete vlan

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

Example usage:

To remove the VLAN "v1":

```
DES-3528:5#delete vlan v1
Command: delete vlan v1

Success.

DES-3528:5#
```

delete vlan vlanid

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

Example usage:

To delete VLAN ID on the Switch:

```
DES-3528:5#delete vlan vlanid 5
Command: delete vlan vlanid 5

Success

DES-3528:5#
```

config vlan

Purpose	Used to add additional ports to a previously configured VLAN, and enable or disable the VLAN advertisement.
Syntax	config vlan <vlan_name 32> { [add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable]}(1)
Description	This command allows the user to add ports to the port list of a previously configured VLAN, and enable or disable the VLAN advertisement. The user can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	<p><vlan_name 32> – The name of the VLAN to which to add ports.</p> <p><i>add</i> – Entering the add parameter will add ports to the VLAN. There are three types of ports to add:</p> <ul style="list-style-type: none"> • <i>tagged</i> – Specifies the additional ports as tagged. • <i>untagged</i> – Specifies the additional ports as untagged. • <i>forbidden</i> – Specifies the additional ports as forbidden <p><i>delete</i> – Deletes ports from the specified VLAN.</p> <p><portlist> – A port or range of ports to add to, or delete from the specified VLAN.</p> <p><i>advertisement [enable disable]</i> – Enables or disables GVRP on the specified VLAN.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DES-3528:5#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DES-3528:5#
```

To delete ports from a VLAN:

```
DES-3528:5#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.

DES-3528:5#
```

config vlan vlanid

Purpose	Used to add additional ports to a previously configured VLAN and enable or disable the VLAN advertisement.
Syntax	config vlan vlanid <vidlist> {[add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable] name <vlan_name 32>}(1)
Description	This command allows you to add or delete ports of the port list of previously configured VLAN(s). You can 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. You can also specify if the VLAN will join GVRP or not with the <i>advertisement</i> parameter. The <i>name</i> parameter allows you to specify the name of the VLAN that needs to be modified.
Parameters	<p><vidlist> – Specifies a range of multiple VLAN IDs to be configured.</p> <p><i>tagged</i> – Specifies the additional ports as tagged.</p> <p><i>untagged</i> – Specifies the additional ports as untagged.</p> <p><i>forbidden</i> – Specifies the additional ports as forbidden.</p> <p><portlist> – A range of ports to add to or delete from the VLAN.</p> <p><i>advertisement</i> – Entering the advertisement parameter specifies if the VLAN should join GVRP or not. There are two parameters:</p> <ul style="list-style-type: none"> ▪ <i>enable</i> – Specifies that the VLAN should join GVRP. ▪ <i>Disable</i> – Specifies that the VLAN should not join GVRP. <p><i>name</i> – 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 and Operator-level users can issue this command.

Example usage:

To config vlan vlanid on the switch:

```
DES-3528:5#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-3528:5#
```

config port_vlan

Purpose	Used to set the ingress checking status, and the sending and receiving GVRP information.
Syntax	config port_vlan [<portlist> all] { gvrp_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 and Operator-level users can issue this command.

Example usage:

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

```
DES-3528:5#config port_vlan 1-4 gvrp_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-3528:5#
```

enable gvrp

Purpose	Used to enable the Generic VLAN Registration Protocol (GVRP).
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 and Operator-level users can issue this command.

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DES-3528:5#enable gvrp
Command: enable gvrp

Success.

DES-3528:5#
```


disable gvrp

Purpose	Used to disable the Generic VLAN Registration Protocol (GVRP).
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 and Operator-level users can issue this command.

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DES-3528:5#disable gvrp
Command: disable gvrp

Success.

DES-3528:5#
```

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 displays summary information about each VLAN including the VLAN ID, VLAN name, the Tagging/Untagging status, and the Member/Non-member/Forbidden status of each port that is a member of the VLAN.
Parameters	<vlan_name 32> – The VLAN name of the VLAN for which to display a summary of settings. <vidlist> – Specifies a list of VLANs by VLAN ID. <portlist> - Specifies the port to be displayed.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```

DES-3528:5#show vlan
Command: show vlan

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

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

VID          : 100       VLAN Name      :
VLAN Type    : Dynamic   Advertisement : Enabled
Member Ports : 8
Static Ports :
Current Tagged Ports : 8
Current Untagged Ports:
Static Tagged Ports  :
Static Untagged Ports :
Forbidden Ports      :

Total Static VLAN Entries : 1
Total GVRP VLAN Entries: 1

DES-3528:5#
    
```

```

DES-3528:5#show vlan ports 1-4
Command: show vlan ports 1-4

Port    VID    Untagged  Tagged  Dynamic  Forbidden
-----  ---    -
1       1       X         -       -        -
2       1       X         -       -        -
3       1       X         -       -        -
4       1       X         -       -        -

DES-3528:5#
    
```

show port_vlan

Purpose	Used to display the ports' VLAN attributes on the Switch.
Syntax	show port_vlan {<portlist>}
Description	This command displays the GVRP status for a port list on the Switch
Parameters	<portlist> – Specifies a range of ports to be displayed. If no parameter specified, system will display all ports GVRP information.
Restrictions	None.

Example usage:

To display GVRP port status:

```
DES-3528:5#show port_vlan 1-10
Command: show port_vlan 1-10
```

Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Disabled	Enabled	All Frames
2	1	Disabled	Enabled	All Frames
3	1	Disabled	Enabled	All Frames
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

create dot1v_protocol_group

Purpose	Used to create a protocol group for protocol VLAN function.
Syntax	create dot1v_protocol_group group_id < id 1-16> group_name <name 32>
Description	This command creates a protocol group for protocol VLAN function.
Parameters	<i>group_id</i> – The ID of a protocol group which is used to identify a set of protocols. <i>group_name</i> – The name of the protocol group. The maximum length is 32 characters.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a protocol group:

```
DES-3528:5#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-3528:5#
```

config dot1v_protocol_group

Purpose	Used to add/delete a protocol to/from a protocol group.
Syntax	config dot1v_protocol_group [group_id <id 1-16> group_name <name 32>][add protocol [ethernet_2 ieee802.3_snap ieee802.3_llc] <protocol_value> delete protocol [ethernet_2 ieee802.3_snap ieee802.3_llc] <protocol_value>]
Description	This command adds/deletes a protocol to/from a protocol group. The selection of a protocol can be a pre-defined protocol type or a user specified protocol type.
Parameters	<p><i>group_id</i> – The id of protocol group which is used to identify a set of protocols.</p> <p><i>group_name</i> – The name of the protocol group. The maximum length is 32 chars.</p> <p><i>protocol_value</i> – 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 'ethernetII', this is a 16-bit (2-octet) hex value. Example: Ipv4 is 800, ipv6 is 86dd, ARP is 806,.. and so on.</p> <p>For 'IEEE802.3 SNAP', this is a 16-bit (2-octet) hex value. Example: Ipv4 is 800, ipv6 is 86dd, ARP is 806,.. and so on. For 'IEEE802.3 LLC', this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair: first octet for Destination Service Access Point (DSAP) and second octet for Source.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a protocol IPv6 to protocol group 1:

```
DES-3528:5#config dot1v_protocol_group group_id 1 add protocol Ethernet_2 86DD
Command: config dot1v_protocol_group group_id 1 add protocol Ethernet_2 86DD

Success.

DES-3528:5#
```

delete dot1v_protocol_group

Purpose	Used to delete a protocol group.
Syntax	delete dot1v_protocol_group [group_id <id 1-16> group_name <name 32> all]
Description	This command deletes a protocol group
Parameters	<p><i>group_id</i> – Specifies the group ID to be deleted.</p> <p><i>group_name</i> – The name of the protocol group. The maximum length is 32 characters.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete protocol group 1:

```
DES-3528:5#delete dot1v_protocol_group group_id 1
Command: delete dot1v_protocol_group group_id 1

Success.

DES-3528:5#
```

show dot1v_protocol_group

Purpose	Used to display the protocols defined in a protocol group.
Syntax	show dot1v_protocol_group {group_id <id 1-16> group_name <name 32>}
Description	This command displays the protocols defined in protocol groups.
Parameters	<i>group_id</i> – Specifies the ID of the group to be displayed if group ID is not specified, all configured protocol groups will be displayed. <i>group_name</i> – The name of the protocol group. The maximum length is 32 characters.
Restrictions	None.

Example usage:

To display the protocol group ID 1:

```
DES-3528:5#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

```
Total Entries: 1
```

```
DES-3528:5#
```

config port dot1v

Purpose	Used to assign the VLAN for untagged packets which ingress from the portlist based on the protocol group configured.
Syntax	config port dot1v ports [<portlist> all] [add protocol_group [group_id <id> group_name <name 32>] [vlan <vlan_name 32> vlanid <id>] {priority <value 0-7>} delete protocol_group [group_id <id 1-16> all]]
Description	This command assigns the VLAN for untagged packets which ingress from the portlist based on the protocol group configured. This assignment can be removed by using 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	<i><portlist></i> – Specifies a range of ports to apply this command. <i>group_id</i> – The id of protocol group which is used to identify a set of protocols. <i>group_name</i> – The name of the protocol group. The maximum length is 32 characters. <i>vlan</i> – Vlan that is to be associated with this protocol group on this port. <i>vlan_id</i> – Specifies the VLAN ID. <i>priority</i> – Specifies the priority to be associated with the packet which has been classified to the specified VLAN by the protocol.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

The example is to assign VLAN marketing-1 for untagged ipv6 packet ingress from port 3.

To configure the group ID 1 on port 3 to be associated with VLAN marketing-1:

```
DES-3528:5#config port dot1v ports 3 add protocol_group group_id 1 vlan marketing_1
Command: config port dot1v ports 3 add protocol_group group_id 1 vlan marketing_1

Success.

DES-3528:5#
```

show port dot1v

Purpose	Used to display the VLAN to be associated with untagged packet ingressed from a port based on the protocol group.
Syntax	show port dot1v{ ports <portlist>}
Description	This command displays the VLAN to be associated with untagged packet ingressed from a port based on the protocol group.
Parameters	<i>portlist</i> – Specifies a range of ports to apply this command.
Restrictions	None.

Example usage:

The example displays the protocol VLAN information for ports 1 – 2:

```
DES-3528:5#show port dot1v ports 1-2
Command: show port dot1v ports 1-2

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

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

[0]Total Entries: 2
DES-3528:5#
```

enable pvid auto_assign

Purpose	Used to enable auto assignment of PVID.
Syntax	enable pvid auto_assign
Description	This command enables the auto-assign of PVID. When this is enabled, PVID will be possibly changed by PVID or VLAN configuration. When user configures a port to VLAN X's untagged membership, this port's PVID will be updated with VLAN X. In the form of VLAN list command, PVID is updated with last item of VLAN list. When user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned with "default VLAN". The default setting is <i>enabled</i> .
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the auto-assign PVID:

```
DES-3528:5#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DES-3528:5#
```

disable pvid auto_assign

Purpose	Used to disable auto assignment of PVID.
Syntax	disable pvid auto_assign
Description	This command disables the auto-assign of PVID. When it is disabled, PVID only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID. The default setting is <i>enabled</i> .
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the auto-assign PVID:

```
DES-3528:5#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DES-3528:5#
```

show pvid auto_assign

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

Example usage:

To display PVID auto-assignment state:

```
DES-3528:5#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled.

DES-3528:5#
```

config gvrp

Purpose	Used to configure the GVRP's timer and its MAC address format for NNI ports when used in Q-in-Q mode.
Syntax	config gvrp [timer [join leave leaveall] < value 100-100000> nni_bpdu_addr [dot1d dot1ad]]
Description	This command is used to set the GVRP's timer and its MAC address format for NNI ports when used in Q-in-Q mode. The default value for Join time is 200 milliseconds; for Leave time is 600 milliseconds; for LeaveAll time is 10000 milliseconds.
Parameters	<p><i>join</i> – Specifies the Join time will be set</p> <p><i>leave</i> – Specifies the Leave time will be set</p> <p><i>leaveall</i> – Specifies the LeaveAll time will be set</p> <p><i>value</i> – The time value will be set. The value range is 100 to 100000 milliseconds. In addition, the Leave time should greater than 2 Join times and the LeaveAll time should greater than Leave time.</p> <p><i>nni_bpdu_addr</i> - Uses to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address or 802.1ad service provider GVRP address.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the Join time to 200 milliseconds:

```
DES-3528:5#config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DES-3528:5#
```

show gvrp

Purpose	Used to display the GVRP global setting and it's timer's value.
Syntax	show gvrp
Description	This command displays GVRP global setting and it's timer's value.
Parameters	None.
Restrictions	None.

Example usage:

To display the timer's value of GVRP:


```
DES-3552:5#show gvrp
Command: show gvrp

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

DES-3528:5#
```

enable vlan_trunk

Purpose	Used to enable the VLAN trunk function.
Syntax	enable vlan_trunk
Description	This command enables the VLAN trunk function. When enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the VLAN trunk:

```
DES-3528:5#enable vlan_trunk
Command: enable vlan_trunk

Success.

DES-3528:5#
```

disable vlan_trunk

Purpose	Used to disable the VLAN trunk function.
Syntax	disable vlan_trunk
Description	This command disables the VLAN trunk function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the VLAN trunk:

```
DES-3528:5#disable vlan_trunk
Command: disable vlan_trunk

Success.

DES-3528:5#
```

config vlan_trunk ports

Purpose	Used to configure a port as a VLAN trunk port.
Syntax	config vlan_trunk ports [<portlist> all] state [enable disable]
Description	This command is used to configure a port as a VLAN trunk port. When a port is configured as a VLAN trunk port, all tagged frames shall be able to pass through this port.
Parameters	<p><portlist> – Specify a range 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 and Operator-level users can issue this command.

Example usage:

To configure VLAN trunk ports:

```
DES-3528:5# config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DES-3528:5#
```

show vlan_trunk

Purpose	Used to display the VLAN trunk configuration.
Syntax	show vlan_trunk
Description	This command displays the VLAN trunk configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the VLAN trunk configuration:

```
DES-3528:5#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk Global Setting
-----
VLAN Trunk Status      : Enabled
VLAN Trunk Member Ports : 1-5

DES-3528:5#
```

VOICE VLAN COMMANDS

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

Command	Parameters
enable voice_vlan	[vlan <vlan_name 32> vlanid <vlanid 1-4094>]
disable voice_vlan	
config voice_vlan priority	<int 0-7>
config voice_vlan oui	[add <macaddr> < macmask> {description <desc 32> } delete <macaddr> < macmask>]
config voice_vlan ports	[<portlist> all] [state [enable disable] mode [auto manual]]
config voice_vlan aging_time	<min1-65535>
config voice_vlan trap_log	[enable disable]
show voice_vlan	
show voice_vlan oui	
show voice_vlan ports	{<portlist>}
show voice_vlan voice_device ports	{<portlist>}

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

enable voice_vlan

Purpose	Used to enable the global voice VLAN function.
Syntax	enable voice_vlan [<vlan_name 32> vlanid <vlanid 1-4094>]
Description	This command is used to enable the global voice VLAN function on the Switch. To enable the voice VLAN, the voice VLAN must be assigned to an existing static 802.1Q VLAN. The VLAN with assigned voice VLAN cannot be deleted. To change the voice VLAN, the user must disable the voice VLAN function first, and then re-issue this command. By default, the global voice VLAN state is <i>disabled</i> .
Parameters	<i><vlan_name 32></i> - Specifies the voice VLAN by VLAN name. <i><vlanid 1-4094></i> - Specifies the voice VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable a voice VLAN:

```
DES-3528:5# enable voice_vlan vlanid 1
Command: enable voice_vlan vlanid 1

Success.

DES-3528:5#
```

disable voice_vlan

Purpose	Used to disable the global voice VLAN function.
Syntax	disable voice_vlan
Description	This command disables the global voice VLAN function on the Switch. When the voice VLAN function is disabled, the voice VLAN will become unassigned.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the voice VLAN:

```
DES-3528:5# disable voice_vlan
Command: disable voice_vlan

Success.
DES-3528:5#
```

config voice_vlan priority

Purpose	Used to configure voice VLAN priority.
Syntax	config voice_vlan priority <int 0-7>
Description	This command is used to configure voice VLAN priority. The voice VLAN priority will be the priority associated with the voice VLAN traffic so as to distinguish the QoS of the voice traffic from data traffic.
Parameters	<int 0-7> - Specifies the priority of the voice VLAN. It ranges from 0 to 7. The default setting is 5.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the voice VLAN priority to 6:

```
DES-3528:5# config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.
DES-3528:5#
```

config voice_vlan oui

Purpose	Used to configure the user defined OUI (Organizationally Unique Identifier) of Voice device for voice VLAN.
Syntax	config voice_vlan oui [add <macaddr> < macmask> {description <desc 32> } delete <macaddr> < macmask>]
Description	This command is used to configure the user-defined OUI for voice traffic. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs. However, the user defined OUI cannot be the same as pre-defined OUI.
Parameters	<p><i>add</i> – Adds a user defined OUI for a voice device vendor.</p> <p><i>delete</i> - Deletes a user defined OUI for a voice device vendor.</p> <p><i><macaddr></i> - Specifies the user difined OUI MAC address.</p> <p><i><macmask></i> - Specifies the user difined OUI MAC address mask.</p> <p><i><desc 32></i> - Specifies the descriptions for the user defined OUI.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a user defined OUI of Voice device:

```
DES-3528:5#config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00
Command: config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00

Success.

DES-3528:5#
```

config voice_vlan ports state

Purpose	Used to enable or disable the voice VLAN function on ports.
Syntax	config voice_vlan ports [<portlist> all] state [enable disable]
Description	This command is used to enable/disable the voice VLAN function on ports.
Parameters	<p><i><portlist></i> – Specifies a range of ports to configure.</p> <p><i>all</i> - Specifies to configure all ports.</p> <p><i>state</i> – Specifies the voice VLAN function state on ports.</p> <ul style="list-style-type: none"> • <i>enable</i> – Enables the voice VLAN function state on ports. • <i>disable</i> - Disables the voice VLAN function state on ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config voice VLAN portlist 4-6 enable:

```
DES-3528:5# config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

DES-3528:5#
```

config voice_vlan ports mode

Purpose	Used to configure per port voice VLAN mode.
Syntax	config voice_vlan ports <portlist> mode [auto manual]
Description	<p>This command is used to configure per port voice VLAN mode as <i>auto</i> or <i>manual</i>. When the mode is <i>auto</i>, the port can become the voice VLAN member port by auto-learning. If the MAC address of the the received packet matches the configured OUI, the port will dynamically become a member port. The dynamic membership will be removed via the aging out mechanism.</p> <p>When the mode is <i>manual</i>, the port needs to be manually added into or removed from the voice VLAN by 802.1Q VLAN configuration command.</p>
Parameters	<p><portlist> – Specifies a range of ports to configure.</p> <p><i>all</i> - Specifies to configure all ports.</p> <p><i>mode</i> – Specifies the voice VLAN mode.</p> <ul style="list-style-type: none"> • <i>auto</i> – If the mode is <i>auto</i>, the port can become the voice VLAN member port by auto-learning. If the MAC address of the received packet matches the configured OUI addresses, the port will dynamically become a member port. The dynamic membership will be removed via the aging out mechanism. • <i>manual</i> - If the mode is set to <i>manual</i>, the port needs to be manually added into or removed from the voice VLAN by 802.1Q VLAN configuration command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set mode auto to voice VLAN ports 3 - 5:

```
DES-3528:5# config voice_vlan ports 3-5 mode auto
Command: config voice_vlan ports 3-5 mode auto

Success.
DES-3528:5#
```

config voice_vlan aging time

Purpose	Used to config voice VLAN aging time.
Syntax	config voice_vlan aging_time <min 1-65535>
Description	<p>This command is used to set the aging time of the voice VLAN. The aging time is used to remove a port from voice VLAN if the port is an dynamic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after the voice VLAN timer expires. If the voice traffic resume before the aging timer expires, the aging timer will be reset.</p>
Parameters	<i>aging_time</i> – Specifies the aging time. It ranges from 1 to 65535.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set 60 minutes as the aging time of voice VLAN:

```
DES-3528:5# config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.
DES-3528:5#
```

config voice_vlan trap_log

Purpose	Used to config trap/log state for voice VLAN.
Syntax	config voice_vlan trap_log [enable disable]
Description	This command is used to configure the trap/log state for voice VLAN. If there is a new voice device detected/ or a port join/leave the voice VLAN dynamically, and the trap/log is enabled, a trap/log will be triggered.
Parameters	<i>enable</i> – Specifies to enable sending the issue of voice VLAN trap and log. <i>disable</i> - Specifies to disable sending the issue of voice VLAN trap and log.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the trap state for voice VLAN:

```
DES-3528:5#config voice_vlan trap_log enable
Command: config voice_vlan trap_log enable

Success.

DES-3528:5#
```

show voice_vlan

Purpose	Used to display voice VLAN global information.
Syntax	show voice_vlan
Description	This command is used to display voice VLAN global information.
Parameters	None.
Restrictions	None.

Example usage:

To display the voice VLAN global information when voice VLAN is enabled:

```
DES-3528:5#show voice_vlan
Command: show voice_vlan

VoiveVLAN State : Enabled
VoiceVID       : 1
VLAN Name      : default
Priority       : 6
Aging Time    : 60 minutes
Trap State     : Enabled
Log State     : Enabled
Member Ports  : 1-28
Dynamic Ports  :

DES-3528:5#
```

show voice_vlan oui

Purpose	Used to display OUI information of the voice VLAN.
Syntax	show voice_vlan oui
Description	This command is used to display OUI information of the voice VLAN.
Parameters	None.
Restrictions	None.

Example usage:

To display the OUI information of voice VLAN:

```
DES-3528:5#show voice_vlan oui
Command: show voice_vlan oui

OUI Address          Mask                Description
-----
00-01-E3-00-00-00    FF-FF-FF-00-00-00  Siemens
00-03-6B-00-00-00    FF-FF-FF-00-00-00  Cisco
00-09-6E-00-00-00    FF-FF-FF-00-00-00  Avaya
00-0A-0B-00-00-00    FF-FF-FF-00-00-00
00-0F-E2-00-00-00    FF-FF-FF-00-00-00  Huawei&3COM
00-60-B9-00-00-00    FF-FF-FF-00-00-00  NEC&Philips
00-D0-1E-00-00-00    FF-FF-FF-00-00-00  Pingtel
00-E0-75-00-00-00    FF-FF-FF-00-00-00  Veritel
00-E0-BB-00-00-00    FF-FF-FF-00-00-00  3COM

Total Entries: 9

DES-3528:5#
```

show voice_vlan ports

Purpose	Used to display the mode and status of voice VLAN ports.
Syntax	show voice_vlan ports {<portlist>}
Description	This command is used to display the mode and status of voice VLAN ports.
Parameters	<portlist> - A range of port to display. If not specified, all ports' information will be displayed.
Restrictions	None.

Example usage:

To display the voice VLAN information of ports 1:1-1:5:

```
DES-3528:5# show voice_vlan ports 1:1-1:5
Command: show voice_vlan ports 1:1-1:5

Ports   Status   Mode
-----
1:1     Enabled  Auto
1:2     Enabled  Auto
1:3     Enabled  Manual
1:4     Enabled  Auto
1:5     Enabled  Auto

DES-3528:5#
```


show voice_vlan voice_device ports

Purpose	Used to show Voice devices that connected to the ports.
Syntax	show voice_vlan voice_device ports {<portlist> }
Description	This command is used to show voice devices that are connected to the ports.
Parameters	<portlist> - A range of port to display. If not specified, all voice-vlan enabled ports will be displayed.
Restrictions	None.

Example usage:

To display the Voice devices that connected to the ports 1:1-1:5:

```
DES-3528:5# show voice_vlan voice_device port 1:1-1:5
```

```
Command: show voice_vlan voice_device ports 1:1-1:5
```

Ports	Voice Device	Start Time	Last Activity Time
1:1	00-E0-BB-00-00-01	2008-10-6 09:00	2008-10-6 10:30
1:1	00-E0-BB-00-00-02	2008-10-6 14:10	2008-10-6 15:00
1:1	00-E0-BB-00-00-03	2008-10-6 14:20	2008-10-6 15:30
1:2	00-03-6B-00-00-01	2008-10-6 17:15	2008-10-6 18:00
1:4	00-E0-75-00-00-02	2008-10-6 18:15	2008-10-6 20:00
1:5	00-01-E3-01-02-03	2008-10-6 18:30	2008-10-6 20:30

```
Total Entries: 6
```

```
DES-3528:5#
```

SUBNET-BASED VLAN COMMANDS

The subnet-based VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create subnet_vlan network	<network_address> [vlan <vlan_name 32> vlanid <vlanid 1-4094>] {priority <value 0-7>}
delete subnet_vlan	[network <network_address> vlan <vlan_name 32> vlanid <vidlist> all]
show subnet_vlan	{ network <network_address> vlan <vlan_name 32> vlanid <vidlist>}
config vlan_precedence ports	<portlist> [mac_based_vlan subnet_vlan]
show vlan_precedence ports	{<portlist>}

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

create subnet_vlan network

Purpose	Used to create a subnet-based VLAN entry.
Syntax	create subnet_vlan network <network_address> [vlan <vlan_name 32> vlanid <vlanid 1-4094>] {priority <value 0-7>}
Description	This command is used to create a subnet-based VLAN entry. A subnet-based VLAN entry is an IP subnet-based VLAN classification rule. If an untagged or priority-tagged IP packet enters a switch port, its source IP address will be compared with the subnet-based VLAN entries. If the source IP matches the subnet entry, the packet will be classified to the VLAN defined for this subnet.
Parameters	<i>network</i> – Specifies an IPv4 network address. The format is ipaddress/prefix length. <i>vlan</i> – The VLAN to be associated with the subnet. You can specify a VLAN name or VLAN ID. The VLAN must be an existing static VLAN. <i>priority</i> – Specifies the priority to be associated with the subnet. It ranges from 0 to 7.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This example shows how to create a subnet-based VLAN entry.

```
DES-3528:5# create subnet_vlan network 172.168.1.1/24 vlan default priority 2
Command: create subnet_vlan network 172.168.1.1/24 vlan default priority 2

Success.

DES-3528:5#
```

delete subnet_vlan

Purpose	Use this command to delete subnet-based VLAN entry.
Syntax	delete subnet_vlan [network <network_address> vlan <vlan_name 32> vlanid <vidlist> all]
Description	This command is used to delete subnet-based VLAN entry.
Parameters	<p><i>network</i> – Specifies an Ipv4 network address. The format is ipaddress/prefix length.</p> <p><i>vlan</i> – The VLAN to be associated with the subnet. You can specify a VLAN name or VLAN ID. The VLAN must be existed static VLAN.</p> <p><i>vlanid</i> – Specifies a list of VLAN ID.</p> <p><i>all</i> – Specifies to delete all subnet-based VLAN entries.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a subnet-based VLAN entry:

```
DES-3528:5#delete subnet_vlan network 172.168.1.1/24
Command: delete subnet_vlan network 172.168.1.1/24

Success.

DES-3528:5#
```

show subnet_vlan

Purpose	Use to display subnet-based VLAN information.
Syntax	show subnet_vlan { network <network_address> vlan <vlan_name 32> vlanid <vidlist> }
Description	This command is used to display subnet-based VLAN information. If no parameter specified, the command will display all subnet-based VLAN entries.
Parameters	<p><i>network</i> – Specifies an Ipv4 network address. The format is ipaddress/prefix length.</p> <p><i>vlan</i> – The VLAN to be associated with the subnet. You can specify a VLAN name or VLAN ID. The VLAN must be existed static VLAN.</p> <p><i>vlanid</i> – Specifies a list of VLAN ID.</p>
Restrictions	None.

Example usage:

To display the subnet-based VLAN:

```
DES-3528:5#show subnet_vlan
Command: show subnet_vlan

IP Address/Subnet mask          VLAN          Priority
-----
172.168.1.0/255.255.255.0      1             0

Total Entries: 1

DES-3528:5#
```

config vlan_precedence ports

Purpose	Use to configure VLAN classification precedence.
Syntax	config vlan_precedence ports <portlist> [mac_based_vlan subnet_vlan]
Description	<p>This command is used to configure VLAN classification precedence on each port. You can specify MAC-based VLAN classification or subnet-based VLAN classification.</p> <p>If a port's VLAN classification is set to MAC-based VLAN precedence and a packet matches both MAC-based VLAN and subnet-based VLAN entry, the packet will be processed based on MAC-based VLAN entry.</p> <p>If a port's VLAN classification is set to subnet-based VLAN precedence and a packet matches both MAC-based and subnet-based VLAN entries, the packet will be processed based on subnet-based VLAN entry.</p>
Parameters	<p><i><portlist></i> – Specify a range of ports to be configured.</p> <p><i>mac_based_vlan</i> – Specifies to precede subnet-based VLAN classification.</p> <p><i>subnet_vlan</i> – Specifies to precede MAC-based VLAN classification.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure subnet-based VLAN classification precedence on port 1:

```
DES-3528:5#config vlan_precedence ports 1 subnet_vlan
Command: config vlan_precedence ports 1 subnet_vlan

Success.

DES-3528:5#
```

show vlan_precedence ports

Purpose	Use to display VLAN classification precedence.
Syntax	show vlan_precedence ports {<portlist>}
Description	This command is used to display VLAN classification precedence.
Parameters	<i><portlist></i> – Specify a port or a range of ports to be configured.
Restrictions	None.

Example usage:

To display the subnet-based VLAN classification precedence:

```
DES-3528:5#show vlan_precedence ports 1
Command: show vlan_precedence ports 1

Port          VLAN Precedence
----          -
1             Subnet VLAN

DES-3528:5#
```

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 the asymmetric VLAN function on the Switch.
Syntax	enable asymmetric_vlan
Description	This command enables the asymmetric VLAN function on the Switch
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable asymmetric VLANs:

```
DES-3528:5#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DES-3528:5#
```

disable asymmetric_vlan

Purpose	Used to disable the asymmetric VLAN function on the Switch.
Syntax	disable asymmetric_vlan
Description	This command disables the asymmetric VLAN function on the Switch
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable asymmetric VLANs:

```
DES-3528:5#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DES-3528:5#
```

show asymmetric_vlan

Purpose	Used to view the asymmetric VLAN state on the Switch.
Syntax	show asymmetric_vlan
Description	This command displays 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-3528:5#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN: Enabled

DES-3528:5#
```

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 1-8> {type [lacp static]}
delete link_aggregation	group_id <value 1-8>
config link_aggregation	group_id <value 1-8> {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 1-8> algorithm}
config lacp_port	<portlist> mode [active passive]
show lacp_port	{<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 1-8> {type[lacp static]}
Description	This command will create a link aggregation group with a unique identifier.
Parameters	<p><i><value></i> – Specifies the group ID. The Switch allows up to eight link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>type</i> – Specify the type of link aggregation used for the group. If the type is not specified the default type is <i>static</i>.</p> <ul style="list-style-type: none"> <i>lacp</i> – 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. <i>static</i> – This designates the aggregated port group as static. Static port groups cannot be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked 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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DES-3528:5#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DES-3528:5#
```

delete link_aggregation

Purpose	Used to delete a previously configured link aggregation group.
Syntax	delete link_aggregation group_id <value 1-8>
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<i><value 1-8></i> – Specifies the group ID. The Switch allows up to eight link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DES-3528:5#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DES-3528:5#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	config link_aggregation group_id <value 1-8> {master_port <port> ports <portlist> state [enable disable] }(1)
Description	This command allows users to configure a link aggregation group that was created with the create link_aggregation command above.
Parameters	<p><i>group_id <value 1-8></i> – Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>master_port <port></i> – 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.</p> <p><i>ports <portlist></i> – Specifies a port or range of ports that will belong to the link aggregation group.</p> <p><i>state [enable disable]</i> – Allows users to enable or disable the specified link aggregation group.</p>
Restrictions	Only Administrator and Operator-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 5 with group members ports 5-7 plus port 9:

```
DES-3528:5#config link_aggregation group_id 1 master_port 5 ports 5-7, 9
Command: config link_aggregation group_id 1 master_port 5 ports 5-7, 9

Success.

DES-3528:5#
```


config link_aggregation algorithm

Purpose	Used to configure the 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 configures 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><i>mac_source</i> – Indicates that the Switch should examine the MAC source address.</p> <p><i>mac_destination</i> – Indicates that the Switch should examine the MAC destination address.</p> <p><i>mac_source_dest</i> – Indicates that the Switch should examine the MAC source and destination addresses</p> <p><i>ip_source</i> – Indicates that the Switch should examine the IP source address.</p> <p><i>ip_destination</i> – Indicates that the Switch should examine the IP destination address.</p> <p><i>ip_source_dest</i> – Indicates that the Switch should examine the IP source address and the destination address.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DES-3528:5#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest
```

Success.

```
DES-3528:5#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the Switch.
Syntax	show link_aggregation {group_id <value 1-8> algorithm}
Description	This command will display the current link aggregation configuration of the Switch.
Parameters	<p><i><value 1-8></i> – Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>algorithm</i> – Allows users to specify the display of link aggregation by the algorithm in use by that group.</p>
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```

DES-3528:5#show link_aggregation
Command: show link_aggregation
Link Aggregation Algorithm = mac_source_dest

Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   : 7
Status        : Enabled
Flooding Port : 7

Total Entries : 1

DES-3528:5#

```

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><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p><i>mode</i> – Select the mode to determine if LACP ports will process LACP control frames.</p> <ul style="list-style-type: none"> <i>active</i> – 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. <i>passive</i> – 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).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```

DES-3528:5#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DES-3528:5#

```

show lacp_port

Purpose	Used to display current LACP port mode settings.
Syntax	show lacp_port {<portlist>}
Description	This command will 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-3528:5#show lacp_port 1-10
```

```
Command: show lacp_port 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-3528:5#
```

IP-MAC-PORT BINDING (IMPB) COMMANDS

The IP network layer uses a four-byte IP 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 white list. If an unauthorized user tries to access an IMPB-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 DES-3528 Series, the maximum number of IP-MAC Binding entries is 511. The creation of authorized IP-MAC pairs can be manually configured by CLI or Web, or can be learned automatically when DHCP snooping is enabled. The function is port-based, meaning a user can enable or disable the function on the individual port.

ACL Mode

Due to some special cases that have arisen with the IP-MAC-Port Binding, this Switch has been equipped with a special ACL Mode for IP-MAC-Port Binding. When enabled, the Switch will create one entry in the Access Profile Table. The entry may only be created if there are at least a Profile ID available on the Switch. If not, when the ACL Mode is enabled, an error message will be prompted to the user. When the ACL Mode is enabled, the Switch will only accept packets from a created entry in the IP-MAC-Port Binding Setting window. All others will be discarded. The function is port-based, meaning a user can enable or disable the function on the individual port.

To configure the ACL mode, the user must first set up IP-MAC-Port binding using the **create address_binding ip_mac ipaddress** command to create an entry. Then the user must enable the mode by entering the **config address_binding ports <portlist> mode acl** command.



NOTE: When configuring the ACL mode function of the IP-MAC-Port Binding function, please pay close attention to previously set ACL entries. Since the ACL mode is enabled, it adds the last available access profile ID to the ACL table, and the first ACL mode entry takes precedence over later entries. This may render some user-defined ACL parameters inoperable due to the overlapping of settings combined with the ACL entry priority (defined by profile ID). For more information on ACL settings, please refer to "[Access Control List \(ACL\) Commands](#)" section in this manual.



NOTE: Once ACL profiles have been created by the Switch through the IP-MAC-Port Binding function, the user cannot modify, delete or add ACL rules to these ACL mode access profile entries. Any attempt to modify, delete or add ACL rules will result in a configuration error as seen in the previous figure.



NOTE: When downloading configuration files to the Switch, be aware of the ACL configurations loaded, as compared to the ACL mode access profile entries set by this function, which may cause both access profile types to experience problems.

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] mode [arp acl]}
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_dhcppkt [enable disable] mode [arp acl] stop_learning_threshold <value 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	
debug address_binding	[event dhcp all]
no debug address_binding	
enable address_binding dhcp_snoop	
disable address_binding dhcp_snoop	
clear address_binding dhcp_snoop binding_entry	ports [<portlist> all]
show address_binding dhcp_snoop	{[max_entry { ports <portlist>} binding_entry {port <port>}]}
config address_binding dhcp_snoop max_entry ports	[<portlist> all] limit [<value 1-50> no_limit]
config address_binding recover_learning ports	[<portlist> all]

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 in the white list.
Syntax	create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> all] mode [arp acl]}
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> <p>mode – This command is used to be compatible with Release 1 CLI firmware.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create address binding entry on the Switch:

```
DES-3528:5#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-3528:5#
```

Once an entry has been created and some IMPB-enabled ports (ACL mode) belong to this entry, the access profile table will look like this:

```
DES-3528:5#show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries:1790
Total Used Rule Entries :2

Access Profile ID: 14                Type : Ethernet IP
=====
Owner      : IP-MAC-Port Binding
MASK Option :
Source MAC      Ethernet Type Source IP Mask
FF-FF-FF-FF-FF-FF      255.255.255.255
-----
-----

Access ID : 1                Mode: Permit                RX Rate(64Kbps)      : no_limit
Ports: 1-5
-----
00-00-00-00-00-04                10.1.1.3
-----

Access ID : 128              Mode: Deny
Ports: 1-5
-----
                                0x800
=====
Unused Entries: 126

DES-3528:5#
```

The **show access_profile** command will display the one access profile created and their corresponding rules for every port on the Switch.

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, if no port is specified it will apply to all ports.</p> <p>all – Specifies that all ports on the switch will be configured for address binding.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure address binding entry on the Switch:

```
DES-3528:5#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-3528:5#
```

config address_binding ip_mac ports

Purpose	Used to configure IMPB settings for specified ports.
Syntax	config address_binding ip_mac ports [<portlist> all] {state [enable {[strict loose]} disable] allow_zeroip [enable disable] forward_dhcp pkt [enable disable] mode [arp acl] stop_learning_threshold <value 0-500>}(1)
Description	<p>This command is used to configure the per-port state of IP-MAC binding on the Switch. If a port has been configured as a group member of an aggregated link, then it cannot enable the IP-MAC binding function.</p> <p>When IMPB is enabled on a port, IP packets and ARP packets received by this port will be checked depending on the setting. The packet will be dropped if its IP-MAC pair does not match the IMPB white list.</p> <p>IMPB allows the user to choose either ARP or ACL mode. In ARP Mode, a switch performs ARP Packet Inspection in which it checks the IP-MAC pairs in ARP packets with the IMPB white list and denies unauthorized ones. An advantage of ARP mode is that it does not consume any ACL rules on the Switch. Nonetheless, since the switch only checks ARP packets, it cannot block unauthorized clients who do not send out ARP packets. In ACL Mode, a switch performs IP Packet Inspection in addition to ARP Packet Inspection. ACL rules will be used to permit statically configured IMPB entries and deny other IP packets with the incorrect IP-MAC pairs. The distinct advantage of ACL Mode is that it ensures better security by checking both ARP Packets and IP Packets. However, doing so requires the use of ACL rules. ACL Mode can be viewed as an enhanced version of ARP Mode because ARP Mode is enabled by default when ACL Mode is selected.</p> <p>There are also two port states: Strict and Loose, and only one state can be selected per port. If a port is set to Strict state, all packets sent to the port are denied (dropped) by default. The Switch will continuously compare all IP and ARP packets it receives on that port with its IMPB entries. If the IP-MAC pair in the packet matches the IMPB entry, the MAC address will be unblocked and subsequent packets sent from this client will be forwarded. On the other hand, if a port is set to Loose state, all packets entering the port are permitted (forwarded) by default. The Switch will continuously compare all ARP</p>

config address_binding ip_mac ports

packets it receives on that port with its IMPB entries. If the IP-MAC pair in the ARP packet does not match the IMPB white list, the MAC address will be blocked and subsequent packets sent from this client will be dropped.

Parameters

state – Configures the address binding port state to enable or disable. When the state is enabled, the port will perform the binding check.

strict – This state provides a stricter method of control. If the user selects this mode, all packets are blocked by the Switch by default. The Switch will compare all incoming ARP and IP Packets and attempt to match them against the IMPB white list. If the IP-MAC pair matches the white list entry, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the Strict state uses more CPU resources from checking every incoming ARP and IP packet, it enforces better security and is thus the recommended setting.

The packet isn't found by the entry, the MAC will be set to block. Other packets will be dropped. The default mode is strict if not specified.

loose – This mode provides a looser way of control. If the user selects loose mode, the Switch will forward all packets by default. However, it will still inspect incoming ARP packets and compare them with the Switch's IMPB white list entries. If the IP-MAC pair of a packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources because the Switch only checks incoming ARP packets. However, it also means that Loose state cannot block users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets.

allow_zeroip – Specifies whether to allow ARP packets with Source IP address 0.0.0.0. When enabled on a port, all ARP packets with a source IP address of 0.0.0.0 is forwarded; when set to disable, they are blocked.

forward_dhcppkt – By default, the Switch will forward all DHCP packets. However, if the port state is set to Strict, all DHCP packets will be dropped. In that case, enable *forward_dhcppkt* so that the port will forward DHCP packets even under Strict state. Enabling this feature also ensures that DHCP snooping works properly.

mode – select to port to use *ARP* mode or *ACL* mode. When a port is under *ACL* mode, the switch will create *ACL* access entry corresponding to the entries of this port. If the port mode changes to *ARP*, all the *ACL* access entries will be deleted automatically. The default mode of the port is *ARP* mode.

stop_learning_threshold <value 0-500> – Enter a stop learning threshold between 0 and 500. Entering 500 means the port will enter the stop learning state after 500 illegal MAC entries and will not allow additional MAC entries, both legal or illegal, to be learned on this port. In the stop learning state, the port will also automatically purge all blocked MAC entries on this port. Traffic from legal MAC entries are still forwarded. Entering 0 means no limit has been set and the port will keep learning illegal MAC addresses.

<portlist> – Specifies a port or range of ports to be configured.

all – Specifies all ports on the switch.

Restrictions

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

Example usage:

To enable port 1 address_binding state:

```
DES-3528:5#config address_binding ip_mac ports 1 state enable
```

```
Command: config address_binding ip_mac ports 1 state enable
```

```
Success.
```

```
DES-3528:5#
```

To enable port 1 address_binding state and set mode to acl:


```
DES-3528:5#config address_binding ip_mac ports 1 state enable mode acl
Command: config address_binding ip_mac ports 1 state enable mode acl

Success.

DES-3528:5#
```

To enable port 1 address_binding state and set stop_learning_threshold to 60:

```
DES-3528:5#config address_binding ip_mac ports 1 state enable
stop_learning_threshold 60
Command: config address_binding ip_mac ports 1 state enable
stop_learning_threshold 60

Success.

DES-3528:5#
```

show address_binding

Purpose	Used to show address binding entries, blocked MAC entries, and port status.
Syntax	show address_binding {[ip_mac [all ipaddress <ipaddr> mac_address <macaddr>] blocked [all vlan_name <vlan_name> mac_address <macaddr>] ports]}
Description	This command is used to display IP-MAC-Port Binding entries. Three different kinds of information can be viewed. <ul style="list-style-type: none"> • <i>ip_mac</i> – Address Binding entries can be viewed by entering the MAC and IP addresses of the device. • <i>blocked</i> – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the MAC address of the device. • <i>ports</i> –Address binding status of all ports can be viewed.
Parameters	<i>all</i> – Displays all IP-MAC-Port binding entries; for Blocked Address Binding entries, <i>all</i> specifies all the blocked VLANs and their bound MAC addresses. <ipaddr> – The IP address of the device where the IP-MAC-Port binding is made. <macaddr> – The MAC address of the device where the IP-MAC-Port binding is made. <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.
Restrictions	None.

Example usage:

To show IP-MAC-Port Binding global configuration:

```
DES-3528:5#show address_binding
Command: show address_binding

Trap/Log      : Disabled
DHCP Snoop    : Disabled

DES-3528:5#
```

To show IP-MAC-Port Binding entries:

```
DES-3528:5#show address_binding ip_mac all
Command: show address_binding ip_mac all

IP Address      MAC Address      Mode  Ports
-----
10.1.1.3        00-00-00-00-00-05  Static  1-28

Total Entries : 1

DES-3528:5#
```

To show IP-MAC-Port Binding blocked MAC entries:

```
DES-3528:5#show address_binding blocked all
Command: show address_binding blocked all

VID  VLAN Name      MAC Address      Port
----
1    default        00-05-5D-0B-AD-A5  1
1    default        00-05-5D-65-76-60  1
1    default        00-0F-EA-13-4F-4A  1
1    default        00-15-E9-85-BD-3F  1
1    default        00-16-36-8A-42-CB  1
1    default        00-16-76-33-FC-88  1
1    default        00-1A-4D-65-FE-A5  1
1    default        00-1B-11-C8-55-CB  1

Total Entries : 8

DES-3528:5#
```

To show IP-MAC-Port Binding ports:

```
DES-3528:5#show address_binding ports
Command: show address_binding ports

Port  State      Mode  Zero IP      DHCP Packet      Stop Learning Threshold/Mode
-----
1     Strict    ACL   Not Allow    Forward          60 /Normal
2     Strict    ACL   Not Allow    Forward          500/Normal
3     Strict    ACL   Not Allow    Forward          500/Normal
4     Strict    ACL   Not Allow    Forward          500/Normal
5     Strict    ACL   Not Allow    Forward          500/Normal
6     Strict    ARP   Not Allow    Forward          500/Normal
7     Strict    ARP   Not Allow    Forward          500/Normal
```

8	Strict	ARP	Not Allow	Forward	500/Normal
9	Strict	ARP	Not Allow	Forward	500/Normal
10	Strict	ARP	Not Allow	Forward	500/Normal
11	Strict	ARP	Not Allow	Forward	500/Normal
12	Strict	ARP	Not Allow	Forward	500/Normal
13	Strict	ARP	Not Allow	Forward	500/Normal
14	Strict	ARP	Not Allow	Forward	500/Normal
15	Strict	ARP	Not Allow	Forward	500/Normal
16	Strict	ARP	Not Allow	Forward	500/Normal
17	Strict	ARP	Not Allow	Forward	500/Normal
18	Strict	ARP	Not Allow	Forward	500/Normal
19	Strict	ARP	Not Allow	Forward	500/Normal
20	Strict	ARP	Not Allow	Forward	500/Normal

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

delete address_binding

Purpose Used to delete IP-MAC-Port Binding entries and blocked MAC entries.

Syntax `delete address_binding [ip_mac [ipaddress <ipaddr> mac_address <macaddr> | all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]`

Description This command is used to delete IP-MAC-Port Binding entries. Two different kinds of information can be deleted.

- *ip_mac* – Individual Address Binding entries can be deleted by entering the MAC and IP addresses of the device. Toggling to *all* will delete all the Address Binding entries.
- *blocked* –Blocked MAC entries(bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the MAC address of the device. To delete all the blocked MAC entries, toggle *all*.

Parameters

- <ipaddr>* – The IP address of the device where the IP-MAC-Port Binding is made.
- <macaddr>* – The MAC address of the device where the IP-MAC-Port Binding is made.
- <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.
- all* – For IP-MAC-Port Binding *all* specifies all the IP-MAC-Port Binding entries; for blocked MAC entries *all* specifies all the blocked MAC entries.

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

Example usage:

To delete an IP-MAC-Port Binding entry on the Switch:

```
DES-3528:5#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-3528:5#
```

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 IMPB. When enabled, the Switch will send a trap / log message when an ARP packet is received that doesn't match the IMPB white list.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable address binding trap log on the Switch:

```
DES-3528:5#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DES-3528:5#
```

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 IMPB. When disabled, the Switch will not send trap / log messages.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable address binding trap log on the Switch:

```
DES-3528:5#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DES-3528:5#
```

debug address_binding

Purpose	Used to configure the address binding debugging feature on the Switch.
Syntax	debug address_binding [event dhcp all]
Description	This command is used to configure the IPMB debugging feature. The debugging feature is disabled by default.
Parameters	<i>event</i> – The Switch will print out the debug messages when an IMPB module receives ARP/IP packets. <i>dhcp</i> –The Switch will print out the debug messages when the IMPB module receives the DHCP packets. <i>all</i> –The Switch will print out all debugging messages.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To open the debug event:

```
DES-3528:5#debug address_binding event
Command: debug address_binding event

Success.

DES-3528:5#
```

no debug address_binding

Purpose	Used to disable IMPB debugging on the Switch.
Syntax	no debug address_binding
Description	This command is used to disable IMPB debugging on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To close the debug:

```
DES-3528:5#no debug address_binding
Command: no debug address_binding

Success.

DES-3528:5#
```

enable address_binding dhcp_snoop

Purpose	Used to enable the DHCP snooping option for IMPB.
Syntax	enable address_binding dhcp_snoop
Description	<p>If DHCP snooping is enabled, the Switch learns IP-MAC pairs by snooping DHCP packets automatically and then saves them to the IP-MAC-Port Binding white list. This enables a hassle-free configuration because the administrator does not need to manually enter each IMPB entry. A prerequisite for this is that the valid DHCP server's IP-MAC pair must be configured on the Switch's IMPB while list first; otherwise the DHCP server packets will be dropped. DHCP snooping is generally considered to be more secure because it enforces all clients to acquire IP through the DHCP server. Additionally, it makes IP Information auditable because clients cannot manually configure their own IP address.</p> <p>Each DHCP-snooped entry is associated with a lease time. When the lease time expires, the expired entry will be removed from this port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address is moved to a different port.</p> <p>In order to avoid conflict where both static entry and DHCP Snooping entry are the same, DHCP Snooping entries will not be created if the IP-MAC entry has already been statically configured.</p>
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the address binding DHCP snooping mode:

```
DES-3528:5#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DES-3528:5#
```

disable address_binding dhcp_snoop

Purpose	Used to disable the DHCP snooping option for IMPB.
Syntax	disable address_binding dhcp_snoop
Description	When the DHCP snoop function is disabled, all of the auto-learned binding entries will be removed.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the address binding DHCP snooping mode:

```
DES-3528:5#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DES-3528:5#
```

clear address_binding dhcp_snoop binding_entry

Purpose	Used to clear DHCP snooping entries on specified ports.
Syntax	clear address_binding dhcp_snoop binding_entry ports [<portlist> all]
Description	This command is used to clear the DHCP snooping entries learned for the specified ports.
Parameters	<i>ports</i> – Specifies the list of ports on which to clear the DHCP snooping entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear address binding DHCP snooping entries:

```
DES-3528:5#clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3
```

Success.

```
DES-3528:5#
```

show address_binding dhcp_snoop

Purpose	Used to show DHCP snooping database.
Syntax	show address_binding dhcp_snoop {[max_entry { ports <portlist>} binding_entry {port <port>}}]
Description	This command is used to display DHCP snooping database.
Parameters	<i>max_entry</i> – Displays the max number of entries which can be learned by dhcp snooping on the specified ports. <i>binding_entry</i> – Displays the DHCP snooping entries on the specified port.
Restrictions	None.

Example usage:

To display address binding DHCP snooping status:

```
DES-3528:5#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop
```

```
DHCP_Snoop : Disabled
```

```
DES-3528:5#
```

To display address binding DHCP snooping entries:



NOTE: “Inactive” indicated that the entry is currently inactive due to port link down.

```
DES-3528:5#show address_binding dhcp_snoop binding_entry
```

```
Command: show address_binding dhcp_snoop binding_entry
```

IP Address	MAC Address	Lease Time(secs)	Port	Status
10.62.58.35	00-0B-5D-05-34-0B	35964	1	Active
10.33.53.82	00-20-c3-56-b2-ef	2590	2	Inactive

```
Total entries : 2
```

```
DES-3528:5#
```

To display the address_binding DHCP snooping max_entry on specified ports:

```
DES-3528:5#show address_binding dhcp_snoop max_entry ports 1-12
```

```
Command: show address_binding dhcp_snoop max_entry ports 1-12
```

Port	Max Entry
1	No Limit
2	No Limit
3	No Limit
4	No Limit
5	No Limit
6	No Limit
7	No Limit
8	No Limit
9	No Limit
10	No Limit
11	No Limit
12	No Limit

```
DES-3528:5#
```

config address_binding dhcp_snoop max_entry ports

Purpose	Used to specify the maximum number of entries which can be dynamically learned (DHCP snooping) by the specified ports.
Syntax	config address_binding dhcp_snoop max_entry ports [<portlist> all] limit [<value 1-50> no_limit]
Description	This command is used to specify the maximum number of DHCP snooping entries on specified ports. By default, the per-port maximum entry has no limit.
Parameters	<i>portlist</i> – Specifies the list of ports to be configured for the DHCP snooping maximum learned entry. <i>limit</i> – Specifies the maximum number.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the maximum number of entries that ports 1-3 can learn to 10:

```
DES-3528:5#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-3528:5#
```

config address_binding recover_learning ports

Purpose	Use to recover a port from the stop learning state to the normal state.
Syntax	config address_binding recover_learning ports [<portlist> all]
Description	This command is used to recover the port back to normal state, under which the port will start learning both illegal and legal MAC addresses again.
Parameters	<i>portlist</i> – Specifies the list of ports to recover from stopped learning mode.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure address binding recover learning ports:

```
DES-3528:5#config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

DES-3528:5#
```

LIMITED IP MULTICAST ADDRESS

The Limited IP Multicast command 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 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> vlanid <vidlist>] {[add delete] [profile_id <value 1-24> profile_name <name 1-32>] access [permit deny]} (1)
show limited_multicast_addr	[ports <portlist> vlanid <vidlist>]
config max_mcast_group	[ports <portlist> vlanid <vidlist>] {max_group [<value 1-1024> infinite] action [drop replace]} (1)
show max_mcast_group	[ports <portlist> vlanid <vidlist>]

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

create mcast_filter_profile profile_id

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 configures a multicast address profile. Multiple ranges of multicast addresses can be defined in the profile.
Parameters	<i>profile_id</i> – ID of the profile. The range is 1 to 24. <name 1-32> – Provides a meaningful description for the profile.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a multicast filter profile:

```
DES-3528: 5#create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

DES-3528:5#
```

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 allows the user to add or delete a range of multicast IP addresses previously defined.
Parameters	<i>profile_id</i> – ID of the profile. The range is 1 to 24. <i>profile_name</i> – Provides a meaningful description for the profile. <i>mcast_address_list</i> – List of the multicast addresses to be put in the profile. You can either specify a single multicast IP address or a range of multicast addresses using
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config a multicast filter profile:

```
DES-3528: 5#config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.1
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.1

Success.

DES-3528:5#
```

delete mcast_filter_profile profile_id

Purpose	Used to delete a multicast address profile.
Syntax	delete mcast_filter_profile profile_id [<value 1-24> all]
Description	This command deletes a multicast address profile
Parameters	<i>profile_id</i> – ID of the profile <i>all</i> – All multicast address profiles will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a multicast filter profile:

```
DES-3528: 5#delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3

Success.

DES-3528:5#
```

delete mcast_filter_profile profile_name

Purpose	Used to delete a multicast profile name.
Syntax	delete mcast_filter_profile profile_name <name 1-32>
Description	This command deletes a multicast profile.
Parameters	<i>profile_name <name 1-32 ></i> – Name of the profile.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a multicast filter profile profile name:

```
DES-3528: 5#delete mcast_filter_profile profile_name 123
Command: delete mcast_filter_profile profile_name 123
```

Success.

```
DES-3528:5#
```

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 displays the defined multicast address profiles.
Parameters	<i>profile_id</i> – ID of the profile if not specified all profiles will be displayed. <i>profile_name</i> <name 1-32 > – Name of the profile if not specified all profiles will be displayed.
Restrictions	None

Example usage:

To display a multicast filter profile:

```
DES-3528: 5#show mcast_filter_profile
Command: show mcast_filter_profile
```

Profile ID	Name	Multicast Addresses
----	-----	-----
1	MOD	234.1.1.1 - 238.244.244.244
2	customer	224.19.62.34 - 224.19.162.200

Total Profile Count : 2

```
DES-3528:5#
```

config limited_multicast_addr

Purpose	Used to configure the multicast address filtering function on a port.
Syntax	config limited_multicast_addr [ports <portlist> vlanid <vidlist>] {[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 assigned to a port, the filtering function is not effective. When the function is configured on a port, it limits the multicast group that hosts can join through the operation of IGMP.
Parameters	<i><portlist></i> – A range of ports to config the multicast address filtering function. <i><vidlist></i> – A range of VLAN IDs to config the multicast address filtering function. <i>add</i> – Add a multicast address profile to a port. <i>delete</i> – Delete a multicast address profile to a port. <i>profile_id</i> – A profile to be added to or deleted from the port. <i>profile_name <name 1-32></i> – The name of the profile. <i>permit</i> – Specifies that the multicast packet that matches the addresses defined in the profiles will be permitted. The default mode is permit. <i>deny</i> – Specifies that the multicast packet that matches the addresses defined in the profiles will be denied.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config port 1,3 to set the multicast address profile 2:

```
DES-3528: 5#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-3528:5#
```

show limited_multicast_addr

Purpose	Used to show per-port Limited IP multicast address range.
Syntax	show limited_multicast_addr [ports <portlist> vlanid <vidlist>]
Description	This command shows limited multicast address on a per port or per VID basis. When the function is configured on a port or VLAN, it limits the multicast groups that hosts can join through the operation of IGMP snooping function and layer 3 function.
Parameters	<i><portlist></i> – A range of ports to show the limited multicast address configuration.
Restrictions	None.

Example usage:

To show a limited multicast address range:

```
DES-3528: 5#show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Port      : 1
Access    : Deny

Profile ID      Name                Multicast Addresses
-----
      1         customer          224.19.62.34 - 224.19.162.200

Port      : 3
Access    : Deny

Profile ID      Name                Multicast Addresses
-----
      1         customer          224.19.62.34 - 224.19.162.200

DES-3528:5#
```

config max_mcast_group

Purpose	Used to configure the maximum number of multicast groups that a port can join.
Syntax	config max_mcast_group [ports <portlist> vlanid <vidlist>] {max_group [<value 1-1024> infinite] action [drop replace]} (1)
Description	This command configures the maximum number of multicast groups that a port can join.
Parameters	<p><portlist> – A range of ports to config the max_mcast_group</p> <p><vidlist> – A range of VLAN IDs to config the max_mcast_group.</p> <p>max_group – Specifies the maximum number of the multicast groups. The range is from 1 to 1024 or infinite. Infinite is the default setting.</p> <p>action – Specifies the action to handle the newly learned group when the register is full.</p> <p> drop – The newly learned group will be dropped.</p> <p> replace – The newly learned group will replace the eldest group in the register table.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the maximum number of multicast groups:

```
DES-3528: 5#config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DES-3528:5#
```

show max_mcast_group

Purpose	Used to display the max number of multicast groups that a port can join.
Syntax	show max_mcast_group [ports <portlist> vlanid <vidlist>]
Description	This command display the max number of multicast groups that a port can join.
Parameters	<portlist> – A range of ports to display the max number of multicast groups. <vidlist> – A range of VLAN IDs to display the max number of multicast groups.
Restrictions	None.

Example usage:

To display the maximum number of multicast groups:

```
DES-3528:5#show max_mcast_group ports 1,3
```

```
Command: show max_mcast_group ports 1,3
```

Port	Max Multicast Group Number	Action
-----	-----	-----
1	Infinite	Drop
3	Infinite	Drop

```
Total Entries: 2
```

```
DES-3528:5#
```

BASIC IP COMMANDS

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

Command	Parameters
config ipif	<ipif_name 12> [{ ipaddress <network_address> vlan <vlan_name 32> state [enable disable] proxy_arp [enable disable] {local [enable disable]}}(1) bootp dhcp]
create ipif	<ipif_name 12> {<network_address>} <vlan_name 32> {state [enable disable] proxy_arp[enable disable] {local [enable disable]}}
delete ipif	[<ipif_name 12> all]
show ipif	{<ipif_name 12>}
enable ipif	[<ipif_name 12> all]
disable ipif	[<ipif_name 12> all]

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

config ipif

Purpose	Used to configure the IP interface.
Syntax	config ipif <ipif_name 12> [{ ipaddress <network_address> vlan <vlan_name 32> state [enable disable] proxy_arp [enable disable] {local [enable disable]}}(1) bootp dhcp]
Description	This command is used to configure the IP interface on the Switch.
Parameters	<p><i><ipif_name 12></i> – Enter an alphanumeric string of up to 12 characters to identify this IP interface.</p> <p><i>ipaddress <network_address></i> – 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><i><vlan_name 32></i> – The name of the VLAN corresponding to the System IP interface.</p> <p><i>state [enable disable]</i> – Allows users to enable or disable the IP interface.</p> <p><i>proxy_arp [enable disable]</i> – Allows users to enable or disable the proxy ARP function. The default setting is <i>Disabled</i>.</p> <p><i>local [enable disable]</i> - Controls whether the system provides the proxy reply for the ARP packets destined for IP address located in the same subnet as the received interface. When proxy ARP is enabled for an interface, the system will reply the ARP query destined for IP address located in a different IP subnet from the interface IP. For ARP packets destined for IP address located in the same IP subnet as the interface IP, the system will check this setting to determine whether to reply. The default setting is <i>Disabled</i>.</p> <p><i>bootp</i> – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface.</p> <p><i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface. If users are using the autoconfig feature, the Switch becomes a DHCP client automatically so it is not necessary to change the ipif settings.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the IP interface System:


```
DES-3528:5#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DES-3528:5#
```

create ipif

Purpose	Used to create a L3 interface.
Syntax	create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {state [enable disable] proxy_arp[enable disable] {local [enable disable]}}
Description	This command creates a L3 interface. This interface can be configured with IPv4 address. Currently, it has a restriction. An interface can have only one IPv4 address defined.
Parameters	<p><i><ipif_name 12></i> – The name created for the IP interface.</p> <p><i><network_address></i> – The network address for the IP interface to be created.</p> <p><i><vlan_name 32></i> – The name of vlan.</p> <p><i>state</i> – the state of interface.</p> <p><i>proxy_arp [enable disable]</i> – Allows users to enable or disable the proxy ARP function. The default setting is <i>Disabled</i>.</p> <p><i>local [enable disable]</i> - Controls whether the system provides the proxy reply for the ARP packets destined for IP address located in the same subnet as the received interface. When proxy ARP is enabled for an interface, the system will reply the ARP query destined for IP address located in a different IP subnet from the interface IP. For ARP packets destined for IP address located in the same IP subnet as the interface IP, the system will check this setting to determine whether to reply. The default setting is <i>Disabled</i>.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an interface

```
DES-3528:5#create ipif if2 vlan2 state enable
Command: create ipif if2 vlan2 state enable

Success.

DES-3528:5#
```



NOTE: The DES-3528/52 Series does not support cross-VLAN routing. Clients on different VLANs/subnets within the same DES-3528/52 switch need to communicate with each other via an external L3 router or switch.

delete ipif

Purpose	Used to delete an interface.
Syntax	delete ipif [<ipif_name 12> all]
Description	This command deletes an interface or all interfaces. Note that the system interface cannot be deleted.
Parameters	<ipif_name 12> – The name of the deleted IP interface. all – All IPIF except the System IPIF will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IP interface.

```
DES-3528:5#delete ipif if2
Command: delete ipif if2

Success.

DES-3528:5#
```

enable ipif

Purpose	Used to enable the admin state for an interface.
Syntax	enable ipif [<ipif_name 12> all]
Description	This command enables the state for an IPIF. When the state is enabled, the IPv4 processing will be started. When the IPv4 address is configured on the IPIF.
Parameters	<ipif_name 12> – The name of the IP interface. all – All the interface.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the admin state of one interface .

```
DES-3528:5#enable ipif System
Command: enable ipif System

Success.

DES-3528:5#
```

disable ipif

Purpose	Used to disable the admin state for an interface.
Syntax	disable ipif [<ipif_name 12> all]
Description	This command disables the state for an ipif.
Parameters	<ipif_name 12> – The name of the IP interface. all – Specifies all interfaces.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the admin state for an interface.

```
DES-3528:5#disable ipif System
Command: disable ipif System

Success.

DES-3528:5#
```

show ipif

Purpose	Used to display the configuration of an IP interface on the Switch.
Syntax	show ipif {<ipif_name 12>}
Description	This command will display the configuration of an IP interface on the Switch.
Parameters	<ipif_name 12> – The name of the IP interface.
Restrictions	None.

Example usage:

To display IP interface settings.

```
DES-3528:5#show ipif System
Command: show ipif System

IP Interface           : System
VLAN Name              : default
Interface Admin State  : Enabled
IPv4 Address           : 10.24.73.21/8 (Manual) Primary
Proxy ARP              : Disabled (Local : Disabled)

DES-3528:5#
```

MULTICAST VLAN COMMANDS

The 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> [source_port <portlist> untag_source_port <portlist>] tag_member_port <portlist>] state [enable disable] replace_source_ip <ipaddr> remap_priority [<value 0-7> none] {replace_priority}}(1)
show igmp_snooping multicast_vlan_group	{< vlan_name 32> }
delete igmp_snooping multicast_vlan	<vlan_name 32>
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
show igmp_snooping multicast_vlan	{<vlan_name 32>}
config igmp_snooping multicast_vlan forward_unmatched	[disable enable]
create igmp_snooping multicast_vlan_group_profile	<profile_name 1-32>
config igmp_snooping multicast_vlan_group_profile	<profile_name 1-32> [add delete] <mcast_address_list>
delete igmp_snooping multicast_vlan_group_profile	[<profile_name 1-32> all]
show igmp_snooping multicast_vlan_group_profile	{<profile_name 1-32>}
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add delete] profile_name <profile_name 1-32>
show igmp_snooping multicast_vlan_group	{< vlan_name 32> }
create mld_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config mld_snooping multicast_vlan	<vlan_name 32> {[add delete] [member_port <portlist> [source_port <portlist> untag_source_port <portlist>] tag_member_port <portlist>] state [enable disable] replace_source_ip <ipv6addr> remap_priority [<value 0-7> none] {replace_priority}}(1)
create mld_snooping multicast_vlan_group_profile	<profile_name 1-32>
config mld_snooping multicast_vlan_group_profile	<profile_name 1-32> [add delete] <mcastv6_address_list>
delete mld_snooping multicast_vlan_group_profile	[<profile_name 1-32> all]
show mld_snooping multicast_vlan_group_profile	{<profile_name 1-32>}
config mld_snooping	<vlan_name 32> [add delete] profile_name <profile_name 1-32>

Command	Parameters
multicast_vlan_group	
show mld_snooping multicast_vlan_group	{<vlan_name 32> }
delete mld_snooping multicat_vlan	<vlan_name 32>
enable mld_snooping multicast_vlan	
disable mld_snooping multicast_vlan	
show mld_snooping multicast_vlan	{<vlan_name 32>}
config mld_snooping multicast_vlan forward_unmatched	[disable enable]

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	This command will create a multicast_vlan. Multiple multicast VLANs can be configured. When creating an ISM VLAN, it cannot duplicate with the VLAN entries in the existing 802.1Q VLAN database. The ISM VLAN snooping function can co-exist with the 1Q VLAN snooping function.
Parameters	<p><i><vlan_name></i> – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.</p> <p><i>vlanid</i> – The VLAN ID of the multicast VLAN to be create. The range is 2-4094.</p> <p><i>remap_priority</i> – The remap priority value (0 to 7) is associated with the data traffic to be forwarded on the multicast VLAN. If <i>None</i> is specified, the packet’s original priority will be used. The default setting is <i>none</i>.</p> <p><i>replace_priority</i> - 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 and Operator-level users can issue this command.

Example usage:

To create IGMP snoop multicast VLAN mv12:

```
DES-3528:5#create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2
Success.

DES-3528:5#
```

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> [source_port <portlist> untag_source_port <portlist>] tag_member_port <portlist>] state [enable disable] replace_source_ip <ipaddr> remap_priority [<value 0-7> none] { replace_priority}}(1)
Description	<p>This command allows you to add a untagged member port, a tagged member port, a untagged source port and a tagged source port to the port list. The untagged member port and the untagged source port will automatically become the untagged members of the multicast VLAN, the tagged member port and the tagged source port will automatically become the tagged members of the multicast VLAN. To change the port list, the Switch will add or delete the port list that user entered, and update the previous port list.</p> <p>The member port list and source port list cannot overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN.</p> <p>Before configuring the multicast VLAN member port by using this command, the multicast VLAN must be created first.</p>
Parameters	<p><i><vlan_name32></i> – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.</p> <p><i>member_port</i> – Adds a range of member ports to the multicast VLAN. They will become the untagged member port of the IGMP multicast VLAN.</p> <p><i>source_port</i> – Adds a range of source ports to the multicast VLAN.</p> <p><i>untag_source_port</i> – Adds a range of untagged source ports to the multicast VLAN.</p> <p><i>tag_member_port</i> – Specifies the tagged member port of the IGMP multicast VLAN.</p> <p><i>state</i> – enable or disable multicast VLAN for the chosen VLAN.</p> <p><i>replace_source_ip</i> – With the IGMP snooping function, the IGMP report packet sent by the host will be forwarded to the source port. Before the forwarding of the packet, the source IP address in the join packet needs to be replaced by this IPv4 address.</p> <p><i>remap_priority</i> – Associates the remap priority value (0 to 7) with the data traffic and is forwarded on the multicast VLAN. If <i>none</i> is specified, the packet's original priority will be used. The default setting is <i>none</i>.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IGMP snoop multicast VLAN:

```
DES-3528:5#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-3528:5#
```

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	<i>vlan_name</i> – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters.
Restrictions	None.

Example usage:

To display the multicast groups configured for a multicast VLAN.

```
DES-3528:5#show igmp_snooping multicast_vlan_group v1
Command: show igmp_snooping multicast_vlan_group v1
```

VLAN Name	VLAN ID	Multicast Group Profiles
v1	3	

```
DES-3528:5#
```

delete igmp_snooping multicast_vlan

Purpose	Used to delete a multicast VLAN.
Syntax	delete igmp_snooping multicast_vlan <vlan_name 32>
Description	This command allows you to delete multicat_vlan.
Parameters	<i>vlan_name</i> – The name of the multicast VLAN to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IGMP snoop multicast VLAN:

```
DES-3528:5#delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicast_vlan v1
```

Success.

```
DES-3528:5#
```

enable igmp_snooping multicast_vlan

Purpose	Used to enable the multicast VLAN function.
Syntax	enable igmp_snooping multicast_vlan
Description	This command controls the multicast VLAN function. The ISM VLAN will take effect when IGMP snooping multicast VLAN is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable IGMP snoop multicast VLAN:

```
DES-3528:5#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan
```

Success.

```
DES-3528:5#
```

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 IGMP snooping multicast VLAN function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable IGMP snoop multicast VLAN:

```
DES-3528:5#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan
```

```
Success.
```

```
DES-3528:5#
```

show igmp_snooping multicast_vlan

Purpose	Used to show the information of multicast VLAN.
Syntax	show igmp_snooping multicast_vlan {<vlan_name 32>}
Description	This command allows you to show the information of multicast VLAN.
Parameters	<vlan_name> – The name of the multicast VLAN to be shown.
Restrictions	None.

Example usage:

To display IGMP snoop multicast VLAN:


```

DES-3528:5#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

ISM VLAN Global State      : Disabled

VLAN Name                   :mul
VID                         :2

Member(Untagged) Ports     :
Tagged Member Ports        :
Source Ports                :
Untagged Source Ports      :
Status                      :Disabled
Replace Source IP          : 0.0.0.0
Remap Priority              :None

VLAN Name                   :v1
VID                         :3

Member(Untagged) Ports     :
Tagged Member Ports        :
Source Ports                :
Untagged Source Ports      :
Status                      :Disabled
CTRL+C  ESC  q Quit  SPACE  n Next Page  ENTER Next Entry  a All
    
```

config igmp_snooping multicast_vlan forward_unmatched

Purpose	Used to configure forwarding or dropping of the multicast VLAN unmatched packet.
Syntax	config igmp_snooping multicast_vlan forward_unmatched [disable enable]
Description	When the Switch receives a tagged IGMP group packet, if the VID in the tagged packet belongs to a multicast VLAN and the group does not match all profiles, then the configuration takes effect and the packet will be forwarded or dropped based on the setting. By default, the packet will be dropped.
Parameters	<i>enable</i> – The packet will be forwarded. <i>disable</i> – The packet will be dropped.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure IGMP snooping multicast VLAN forward:

```

DES-3528:5# config igmp_snooping multicast_vlan forward_unmatched enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DES-3528:5#
    
```

create igmp_snooping multicast_vlan_group_profile

Purpose	Used to create an IGMP multicast VLAN group profile on the switch.
Syntax	create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>
Description	This command is used to create an IGMP multicast VLAN group profile on the switch. The profile name used for IGMP snooping must be unique.
Parameters	<profile_name 32> – Specifies the IGMP multicast VLAN group profile name, max length is 32.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IGMP multicast VLAN group profile "g1":

```
DES-3528:5#create igmp_snooping multicast_vlan_group_profile g1
Command: create igmp_snooping multicast_vlan_group_profile g1

Success.

DES-3528:5#
```

config igmp_snooping multicast_vlan_group_profile

Purpose	Used to configure an IGMP snooping multicast group profile on the Switch, and to add or delete multicast address for the profile.
Syntax	config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add delete] <mcast_address_list>
Description	This command configures an IGMP multicast VLAN group profile on the Switch, and can add or delete multicast addresses for the profile.
Parameters	<p><profile_name 32> – Specifies the IGMP multicast VLAN group profile name, max length is 32.</p> <p>[add delete] – Add or delete IGMP multicast address list to or from this multicast VLAN group profile</p> <p><mcast_address_list> – Specifies the IGMP multicast addresses to be configured. It can be a continuous single multicast addresses, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, or a multicast address range, such as 225.1.1.1 - 225.2.2.2, or both of them, such as 225.1.1.1, 225.1.1.18 - 225.1.1.20.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add IGMP multicast address or range to a profile:

```
DES-3528:5#config igmp_snooping multicast_vlan_group_profile g1 add 235.2.2.1-23
5.2.2.2
Command: config igmp_snooping multicast_vlan_group_profile g1 add 235.2.2.1-235.
2.2.2

Success.

DES-3528:5#
```

delete igmp_snooping multicast_vlan_group_profile

Purpose	Used to delete an IGMP multicast VLAN group profile on the switch.
Syntax	delete igmp_snooping multicast_vlan_group_profile [<profile_name 1-32> all]
Description	This command deletes an IGMP multicast VLAN group profile on the switch.
Parameters	<p><profile_name 32> – Specifies the IGMP multicast VLAN profile name, max length is 32.</p> <p>all – All IGMP multicast VLAN group profile will be deleted.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the IGMP multicast VLAN group profile "g1":

```
DES-3528:5#delete igmp_snooping multicast_vlan_group_profile g1
Command: delete igmp_snooping multicast_vlan_group_profile g1

Success.

DES-3528:5#
```

show igmp_snooping multicast_vlan_group_profile

Purpose	Used to show the information about an IGMP multicast VLAN group profile on the Switch.
Syntax	show igmp_snooping multicast_vlan_group_profile {<profile_name 1-32>}
Description	This command is used to show the information about an IGMP multicast VLAN group profile on the Switch.
Parameters	{<profile_name 32>} – Specifies the IGMP multicast VLAN profile name, max length is 32. If not specified, all IGMP multicast VLAN group profiles will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the IGMP multicast VLAN group profile:

```
DES-3528:5#show igmp_snooping multicast_vlan_group_profile
```


```
Command: show igmp_snooping multicast_vlan_group_profile
```

Profile Name	Multicast Addresses
-----	-----
g1	235.2.2.1-235.2.2.2

```
Total Entries: 1
```

```
DES-3528:5#
```

config igmp_snooping multicast_vlan multicast_group

Purpose	Used to bind a multicast group profile to a multicast VLAN. The binding profile will affect the group joined to the multicast VLAN.
Syntax	config igmp_snooping multicast_vlan_group <vlan_name 32> [add delete] profile_name <profile_name 1-32>
Description	After binding a profile to a multicast VLAN, when a multicast group attempt to join this multicast VLAN member port, the group cannot join this multicast VLAN if the group does not belong to the range of binding profile.
	 NOTE: Multiple profiles can be added to a multicast VLAN.
Parameters	<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><i>add</i> – Used to associate a profile to a multicast VLAN.</p> <p><i>delete</i> – Used to de-associate a profile from a multicast VLAN.</p> <p><profile_name 32> – The name of the IGMP multicast VLAN group profile to be associated or de- associated to the specified multicast VLAN.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To associate an IGMP multicast VLAN group profile “g1” to IGMP multicast VLAN “mv1”:

```
DES-3528:5#config igmp_snooping multicast_vlan_group mv1 add profile_name g1
Command: config igmp_snooping multicast_vlan_group mv1 add profile_name g1

Success.

DES-3528:5#
```

show igmp_snooping multicast_vlan_group

Purpose	Used to display the multicast group profiles configured for the specified IGMP multicast VLAN.
Syntax	show igmp_snooping multicast_vlan_group {< vlan_name 32> }
Description	This command is used to display the multicast group profiles configured for the specified IGMP multicast VLAN.
Parameters	<i>vlan_name</i> – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters. If not specified, all Ipv4 multicast VLAN groups will be displayed.
Restrictions	None.

Example usage:

To display the multicast group profiles configured for an IGMP multicast VLAN.

```
DES-3528:5#show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group

VLAN Name                VLAN ID  Multicast Group Profiles
-----
mv1                       2        g1

DES-3528:5#
```

create mld_snooping multicast_vlan

Purpose	Used to create an MLD multicast VLAN
Syntax	create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>
Description	This command will create a MLD multicast_vlan. Multiple multicast VLANs can be configured. When creating MLD multicast VLAN, it cannot duplicate with the VLAN entries in the existing 802.1Q VLAN database. The MLD Multicast VLAN snooping function co-exists with the 1Q VLAN snooping function.
Parameters	<i><vlan_name></i> – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters. <i>vlanid</i> – The VLAN ID of the multicast VLAN to be create. The range is 2-4094.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create MLD multicast VLAN mv1:

```
DES-3528:5#create mld_snooping multicast_vlan mv1 2
Command: create mld_snooping multicast_vlan mv1 2

Success.

DES-3528:5#
```

config mld_snooping multicast_vlan

Purpose	Used to configure the parameter of the specific MLD multicast VLAN.
Syntax	config mld_snooping multicast_vlan <vlan_name 32> {[add delete] [member_port <portlist> [source_port <portlist> untag_source_port <portlist>] tag_member_port <portlist>] state [enable disable] replace_source_ip <ipv6addr> remap_priority [<value 0-7> none] { replace_priority}}(1)
Description	<p>This command allows you to add a untagged member port, a tagged member port, a untagged source port and a tagged source port to the port list. The untagged member port and the untagged source port will automatically become the untagged members of the multicast VLAN, the tagged member port and the tagged source port will automatically become the tagged members of the multicast VLAN. To change the port list, the Switch will add or delete the port list that user entered, and update the previous port list.</p> <p>The member port list and source port list cannot overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN.</p> <p>Before configuring the multicast VLAN member port by using this command, the multicast VLAN must be created first.</p>
Parameters	<p><i><vlan_name32></i> – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.</p> <p><i>member_port</i> – Adds a range of member ports to the multicast VLAN. They will become the untagged member port of the MLD multicast VLAN.</p> <p><i>source_port</i> – Adds a range of source ports to the multicast VLAN.</p> <p><i>untag_source_port</i> – Adds a range of untagged source ports to the multicast VLAN. The PVID of the untag source port will be automatically changed to the multicast VLAN. It shall be only one kind of source port, tag or untag for an ISM VLAN.</p> <p><i>tag_member_port</i> – Specifies the tagged member port of the MLD multicast VLAN.</p> <p><i>state</i> – enable or disable multicast VLAN for the chosen VLAN.</p> <p><i>replace_source_ip</i> – With the MLD snooping function, the MLD report packet sent by the host will be forwarded to the source port. Before the forwarding of the packet, the source IP address in the join packet needs to be replaced by this IPv6 address.</p> <p><i>remap_priority</i> – Associates the remap priority value (0 to 7) with the data traffic and is forwarded on the multicast VLAN. If <i>none</i> is specified, the packet's original priority will be used. The default setting is <i>none</i>.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config MLD multicast VLAN mv1:

```
DES-3528:5#config mld_snooping multicast_vlan mv1 add member_port 1,3 state enable
Command: config mld_snooping multicast_vlan mv1 add member_port 1,3 state enable

Success.

DES-3528:5#
```

create mld_snooping multicast_vlan_group_profile

Purpose	Used to create an MLD multicast VLAN group profile on the switch.
Syntax	create mld_snooping multicast_vlan_group_profile <profile_name 1-32>
Description	This command is used to create an MLD multicast VLAN group profile on the switch. The maximum supported number of multicast VLAN group profiles is project dependent. The profile name used for mld snooping must be unique.
Parameters	<profile_name 32> – Specifies the MLD multicast VLAN group profile name, max length is 32
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an MLD multicast VLAN group profile "g1":

```
DES-3528:5#create mld_snooping multicast_vlan_group_profile g1
Command: create mld_snooping multicast_vlan_group_profile g1

Success.

DES-3528:5#
```

config mld_snooping multicast_vlan_group_profile

Purpose	Used to configure an MLD multicast VLAN group profile on the switch, to add or delete multicast address for the profile.
Syntax	config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add delete] <mcastv6_address_list>
Description	This command configures an MLD multicast VLAN group profile on the switch, and can add or delete multicast addresses for the profile.
Parameters	<profile_name 32> – Specifies the MLD multicast VLAN group profile name, max length is 32. [add delete] – Add or delete MLD multicast address list to or from this multicast VLAN group profile <mcastv6_address_list> – Specifies the MLD multicast addresses to be configured. It can be a continuous single multicast addresses, such as FF12::1, FF12::3, FF12::8, or a multicast address range, such as FF12::1- FF12::12, or both of them, such as FF12::1, FF12::18-FF12::20.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add 225.1.1.1 to 226.1.1.1 to MLD multicast VLAN group profile "g1":

```
DES-3528:5#config mld_snooping multicast_vlan_group_profile g1 add FF12::1-FF12::2
Command: config mld_snooping multicast_vlan_group_profile g1 add FF12::1-FF12::2

Success.

DES-3528:5#
```

delete mld_snooping multicast_vlan_group_profile

Purpose	Used to delete an MLD multicast VLAN group profile on the switch.
Syntax	delete mld_snooping multicast_vlan_group_profile [<profile_name 1-32> all]
Description	This command deletes an MLD multicast VLAN group profile on the switch.
Parameters	<profile_name 32> – Specifies the MLD multicast VLAN profile name, max length is 32. all – All MLD multicast VLAN group profile will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the MLD multicast VLAN group profile "g1":

```
DES-3528:5#delete mld_snooping multicast_vlan_group_profile g1
Command: delete mld_snooping multicast_vlan_group_profile g1

Success.

DES-3528:5#
```

show mld_snooping multicast_vlan_group_profile

Purpose	Used to show the information about an MLD multicast VLAN group profile on the switch.
Syntax	show mld_snooping multicast_vlan_group_profile {<profile_name 1-32>}
Description	This command is used to show the information about an MLD multicast VLAN group profile on the switch.
Parameters	{<profile_name 32>} – Specifies the MLD multicast VLAN profile name, max length is 32. If not specified, all MLD multicast VLAN group profiles will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the MLD multicast VLAN group profile:


```
DES-3528:5#show mld_snooping multicast_vlan_group_profile
Command: show mld_snooping multicast_vlan_group_profile

Profile Name                Multicast Addresses
-----
g1                          FF12::1-FF12::2

Total Entry: 1

DES-3528:5#
```


config mld_snooping multicast_vlan multicast_group

Purpose	Used to bind a multicast group profile to a multicast VLAN. The binding profile will affect the group joined to the multicast VLAN.
Syntax	config mld_snooping multicast_vlan_group <vlan_name 32> [add delete] profile_name <profile_name 1-32>
Description	After binding a profile to a multicast VLAN, when a multicast group attempt to join this multicast VLAN member port, the group cannot join this multicast VLAN if the group does not belong to the range of binding profile.
	 NOTE: Multiple profiles can be added to a multicast VLAN.
Parameters	<p><i><vlan_name 32></i> – 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><i>add</i> – Used to associate a profile to a multicast VLAN.</p> <p><i>delete</i> – Used to de-associate a profile from a multicast VLAN.</p> <p><i><profile_name 32></i> – The name of the MLD multicast VLAN group profile to be associated or de-associated to the specified multicast VLAN.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To associate an MLD multicast VLAN group profile “g1” to MLD multicast VLAN “mv1”:

```
DES-3528:5#config mld_snooping multicast_vlan_group mv1 add profile_name g1
Command: config mld_snooping multicast_vlan_group mv1 add profile_name g1

Success.

DES-3528:5#
```

show mld_snooping multicast_vlan_group

Purpose	Used to display the multicast group profiles configured for the specified MLD multicast VLAN.
Syntax	show mld_snooping multicast_vlan_group {< vlan_name 32> }
Description	This command is used to display the multicast group profiles configured for the specified MLD multicast VLAN.
Parameters	<i>vlan_name</i> – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters. If not specified, all IPv6 multicast VLAN groups will be displayed.
Restrictions	None.

Example usage:

To display the multicast group profiles configured for an MLD multicast VLAN.

```
DES-3528:5#show mld_snooping multicast_vlan_group
```

```
Command: show mld_snooping multicast_vlan_group
```

VLAN Name	VLAN ID	Multicast Group Profiles
mv1	2	g1

```
DES-3528:5#
```

delete mld_snooping multicast_vlan

Purpose	Used to delete an MLD muticast VLAN.
Syntax	delete mld_snooping multicat_vlan <vlan_name 32>
Description	This command allows you to delete an MLD multicast VLAN.
Parameters	<i>vlan_name</i> – The name of the multicast VLAN to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an MLD multicast VLAN:

```
DES-3528:5#delete mld_snooping multicast_vlan mv1
```

```
Command: delete mld_snooping multicast_vlan mv1
```

```
Success.
```

```
DES-3528:5#
```

enable mld_snooping multicast_vlan

Purpose	Used to enable the MLD Multicast VLAN function.
Syntax	enable mld_snooping multicast_vlan
Description	This command is used for the MLD Multicast VLAN to take effect. The MSM VLAN will take effect when MLD snooping multicast VLAN is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable MLD Multicast VLAN:

```
DES-3528:5#enable mld_snooping multicast_vlan
```

```
Command: enable mld_snooping multicast_vlan
```

```
Success.
```

```
DES-3528:5#
```

disable mld_snooping multicast_vlan

Purpose	Used to disable the MLD Multicast VLAN function.
Syntax	disable mld_snooping multicast_vlan
Description	This command is used to disable the MLD Multicast VLAN function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable MLD Multicast VLAN:

```
DES-3528:5#disable mld_snooping multicast_vlan
Command: disable mld_snooping multicast_vlan
```

```
Success.
```

```
DES-3528:5#
```

show mld_snooping multicast_vlan

Purpose	Used to show the information of MLD multicast VLAN.
Syntax	show mld_snooping multicast_vlan {<vlan_name 32>}
Description	This command allows you to show the information of an MLD multicast VLAN.
Parameters	<vlan_name> – The name of the multicast VLAN to be shown. If not specified, all MLD multicast VLANs will be displayed.
Restrictions	None.

Example usage:

To show MLD multicast VLAN:

```
DES-3528:5#show mld_snooping multicast_vlan mv1
Command: show mld_snooping multicast_vlan mv1

MLDM VLAN Global State      : Enabled

VLAN Name                    :mv1
VID                          :2

Member(Untagged) Ports      :1,3
Tagged Member Ports         :
Source Ports                 :
Untagged Source Ports       :
Status                       :Enabled
Replace Source IP           : ::
Remap Priority               :None
```

```
Total Entries: 1
```

```
DES-3528:5#
```

config mld_snooping multicast_vlan forward_unmatched

Purpose	Used to configure forwarding mode for MLD Multicast VLAN unmatched packet.
Syntax	config mld_snooping multicast_vlan forward_unmatched [disable enable]
Description	When the switch receives an MLD packet, it will match the packet against the multicast profile to determine the MLD multicast VLAN to be associated with. If the packet does not match any profiles, the packet will be forwarded or dropped based on the setting. By default, the packet will be dropped.
Parameters	<i>enable</i> – The unmatched packet will be flooded on the VLAN. <i>disable</i> – The unmatched packet will be dropped.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set unmatched packet to be flooded on the VLAN:

```
DES-3528:5#config mld_snooping multicast_vlan forward_unmatched enable
Command: config mld_snooping multicast_vlan forward_unmatched enable

Success.

DES-3528:5#
```

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 <vlan_name 32> vlanid <vidlist> all] { state [enable disable] fast_leave [enable disable] report_suppression [enable disable]} (1)
config igmp_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_member_query_interval <sec 1-25> state [enable disable] version <value 1-3>}(1)
config router_ports	[vlan <vlan_name 32> vlanid <vidlist>] [add delete] <portlist>
config router_ports_forbidden	[vlan <vlan_name 32> vlanid <vidlist>] [add delete] <portlist>
enable igmp_snooping	
show igmp_snooping	{[vlan <vlan_name 32> vlanid <vidlist>]}
disable igmp_snooping	
show igmp_snooping group	{[vlan <vlan_name 32> vlanid <vidlist> ports <portlist>] {<ipaddr>} {data_driven}}
show router_ports	[vlan <vlan_name 32> vlanid <vidlist> all] {[static dynamic forbidden]}
show igmp_snooping rate_limit	[ports <portlist> vlanid <vidlist>]
config igmp_snooping rate_limit	[ports <portlist> vlanid <vidlist>] [<value 1-1000> no_limit]
show igmp_snooping forwarding	{[vlan <vlan_name 32> vlanid <vidlist>]}
create igmp_snooping static_group	[vlan <vlan_name 32> vlanid <vidlist>] <ipaddr>
show igmp_snooping static_group	{[vlan <vlan_name 32> vlanid <vidlist>] < ipaddr >}
delete igmp_snooping static_group	[vlan <vlan_name 32> vlanid <vidlist>] <ipaddr>
config igmp_snooping static_group	[vlan <vlan_name 32> vlanid <vidlist>] <ipaddr> [add delete] <portlist>
show igmp_snooping statistic counter	[vlan <vlan_name 32> vlanid <vidlist> ports <portlist>]
clear igmp_snooping statistic counter	
config igmp_snooping data_driven_learning max_learned_entry	<value 1-1024>
config igmp_snooping data_driven_learning	[all vlan_name <vlan_name> vlanid <vidlist>] { state [enable disable] aged_out [enable disable] expiry_time <sec 1-65535>}(1)
clear igmp_snooping data_driven_group	[all [vlan_name <vlan_name> vlanid <vidlist>] [<ipaddr> all]]

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 <vlan_name 32> vlanid <vidlist> all] { state [enable disable] fast_leave [enable disable] report_suppression [enable disable]}(1)
Description	This command allows the user to configure IGMP snooping on the Switch.
Parameters	<p><i><vlan_name 32></i> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p><i><vidlist></i> – The VIDs of the VLAN for which IGMP snooping is to be configured.</p> <p><i>state [enable disable]</i> – Allows users to enable or disable IGMP snooping for the specified VLAN.</p> <p><i>fast_leave [enable disable]</i> – Allows users to enable or disable IGMP snooping fast leave for the specified VLAN.</p> <p><i>report_suppression [enable disable]</i> – Allows users to enable or disable IGMP snooping report suppression for the specified VLAN.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-3528:5# config igmp_snooping vlan default state enable fast_leave enable
report_suppression disable
```

```
Command: config igmp_snooping vlan default state enable fast_leave enable
report_suppression disable
```

```
Success.
```

```
DES-3528:5#
```

config igmp_snooping querier

Purpose	Used to configure the 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 <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 configures IGMP snooping querier.
Parameters	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured.</p> <p><vidlist> – The VIDs of the VLAN for which IGMP snooping is to be configured.</p> <p>query_interval – Specifies the amount of time in seconds between general query transmissions. the default setting is 125 seconds.</p> <p>max_response_time – The maximum time in seconds to wait for reports from members. 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 IGMP message intervals:</p> <ul style="list-style-type: none"> • Group member interval – Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval – Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count – Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy. <p>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.</p> <p>state – If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). If the state is disabled, then the switch cannot play the role as a querier. Note that if the Layer 3 router connected to the switch provide only the IGMP proxy function but not provide the mutlicast 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.</p> <p>version – The version of the IGMP Query sent by the switch.</p>
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the IGMP snooping querier:

```
DES-3528:5#config igmp_snooping querier vlan default query_interval 125 state enable
Command: config igmp_snooping querier vlan default query_interval 125 state enable
```

Success.

```
DES-3528:5#
```

config router_ports

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

Example usage:

To set up static router ports:

```
DES-3528:5# config router_ports default add 2:1-2:10
Command: config router_ports default add 2:1-2:10

Success.

DES-3528:5#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden multicast router ports.
Syntax	config router_ports_forbidden [vlan <vlan_name 32> vlandid <vidlist>] [add delete] <portlist>
Description	This command allows designation of a port or range of ports as being forbidden to multicast-enabled routers. This will ensure that multicast packets will not be forwarded to this port – regardless of protocol, etc.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p><vidlist> – The VIDs of the VLAN for which IGMP snooping is to be configured.</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 and Operator-level users can issue this command.

Example usage:

To set up forbidden router ports:

```
DES-3528:5#config router_ports_forbidden vlan default add 1-10
Command: config router_ports_forbidden vlan default add 1-10

Success.

DES-3528:5#
```


enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	enable igmp_snooping
Description	This command allows users to enable IGMP snooping on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DES-3528:5#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3528:5#
```

disable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	disable igmp_snooping
Description	This command disables IGMP snooping on the Switch.
Parameters	Entering this command without the parameter will disable igmp snooping on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DES-3528:5#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3528:5#
```

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 will display the current IGMP snooping configuration on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN for which to view the IGMP snooping configuration. <vidlist> – The VIDs of the VLAN for which IGMP snooping is to be configured.
Restrictions	None.

Example usage:

To show IGMP snooping:

```

DES-3528:5#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State           : Enabled
Data Driven Learning Max Entries     : 128

VLAN Name                             : default
Query Interval                        : 125
Max Response Time                     : 10
Robustness Value                      : 2
Last Member Query Interval            : 1
Querier State                         : Enable
Querier Role                          : Querier
Querier IP                            : 10.24.73.21
Querier Expiry Time                   : 0 secs
State                                  : Enable
Fast Leave                            : Enable
Report Suppression                    : Disable
Rate Limit                            : No Limitation
Version                               : 3
Data Driven Learning State            : Enable
Data Driven Learning Aged Out         : Disable
Data Driven Group Expiry Time        : 260

Total Entries: 1

DES-3528:5#

```

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> all] {[static dynamic forbidden]}
Description	This command will display the router ports currently configured on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p><vidlist> – The VIDs of the VLAN for which IGMP snooping is to be configured.</p> <p><i>static</i> – Displays router ports that have been statically configured.</p> <p><i>dynamic</i> – Displays router ports that have been dynamically configured.</p> <p><i>forbidden</i> – Displays router ports that are forbidden.</p>
Restrictions	None.

Example usage:

To display the router ports.

```
DES-3528:5#show router_ports all
```

```
Command: show router_ports all
```

```
VLAN Name           : default
```

```
Static Router Port  : 1-10
```

```
Dynamic Router Port :
```

```
  Router IP         :
```

```
Forbidden Router Port :
```

```
Total Entries: 1
```

```
DES-3528:5#
```

show igmp_snooping group

Purpose	Used to display the current IGMP snooping configuration on the Switch.
Syntax	show igmp_snooping group {[vlan <vlan_name 32> vlanid <vidlist> ports <portlist>] {<ipaddr>}} {data_driven}
Description	This command will display the current IGMP setup currently configured on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN for which to view IGMP snooping group information.</p> <p><vidlist> – The VIDs of the VLAN for which IGMP snooping is to be configured.</p> <p><portlist> – The list of ports for which to view IGMP snooping group information.</p> <p><ipaddr> – To view the information of this specified group.</p> <p>data_driven – To view the groups learnt by data driven only.</p> <p>If no parameter is specified, the system will display all current IGMP snooping groups.</p>
Restrictions	None.

Example usage:

To view the current IGMP snooping group:

```
DES-3528:5#show igmp_snooping group
Command: show igmp_snooping group

Source/Group           : 10.0.0.2/255.0.0.2
VLAN Name/VID          : default/1
Member Ports           : 1-2
UP Time                : 127
Expiry Time            : 120
Filter Mode            : INCLUDE

Source/Group           : 10.0.0.2/255.0.0.3
VLAN Name/VID          : default/1
Member Ports           : 3
UP Time                : 320
Expiry Time            : 120
Filter Mode            : EXCLUDE

Source/Group           : NULL/255.0.0.5
VLAN Name/VID          : default/1
Member Ports           : 4-5
UP Time                : 130
Expiry Time            : 120
Filter Mode            : EXCLUDE

Source/Group           : NULL/255.0.0.5
VLAN Name/VID          : default/1
Member Ports           :
Router Ports           : 24
UP Time                : 1335
Expiry Time            : 120
Filter Mode            : EXCLUDE

DES-3528:5#
```

show igmp_snooping rate_limit

Purpose	Used to show rate limitation.
Syntax	show igmp_snooping rate_limit [ports <portlist> vlanid <vidlist>]
Description	This command shows the rate of IGMP control packet that is allowed per port or VLAN.
Parameters	<portlist> – Specifies a port or range of ports that will be displayed. <vidlist> – Specifies a VLAN or range of VLANs that will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show rate limitation:

```
DES-3528:5#show igmp_snooping rate_limit ports 1
Command: show igmp_snooping rate_limit ports 1

Port      Rate Limitation
-----  -
1         No Limitation

Total Entries: 1

DES-3528:5#
```

config igmp_snooping rate_limit

Purpose	Used to configure rate limitation.
Syntax	config igmp_snooping rate_limit [ports <portlist> vlanid <vidlist>] [<value 1-1000> no_limit]
Description	This command configures the rate of IGMP control packets that are allowed per port or VLAN.
Parameters	<portlist> – Specifies a port or range of ports that will be displayed. <vidlist> – Specifies a VLAN or range of VLANs that will be displayed. <value 1-1000> – Specifies the rate of IGMP control packet that the switch can process on a specific port or VLAN. The rate is specified in packets per second. The packets that exceeds the limited rate will be dropped. The default setting is no_limit. no_limit – Allows users to configure the rate limitation to no limit.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure rate limitation:

```
DES-3528:5#config igmp_snooping rate_limit ports 1 100
Command: config igmp_snooping rate_limit ports 1 100

Success.

DES-3528:5#
```

show igmp_snooping forwarding

Purpose	Used to display the current IGMP snooping forwarding information on the Switch.
----------------	---

show igmp_snooping forwarding

Syntax	show igmp_snooping forwarding {[vlan <vlan_name 32> vlanid <vidlist>]}
Description	This command will display the current IGMP forwarding information on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN for which to view IGMP snooping forwarding information. If not specified, all VLAN's IGMP snooping forwarding information will be displayed.</p> <p><vidlist> – The list of the VLAN IDs for which to view IGMP snooping forwarding information. If not specified, all VLAN's IGMP snooping forwarding information will be displayed.</p>
Restrictions	None.

Example usage:

To view the current IGMP snooping forwarding information:

```
DES-3528:5#show igmp_snooping forwarding
Command: show igmp_snooping forwarding

VLAN Name           : default
Source IP           : *
Multicast Group     : 225.1.1.1
Port Member        : 3

Total Entries : 1
```

create igmp_snooping static_group

Purpose	Used to display the current IGMP snooping static group information on the Switch.
Syntax	create igmp_snooping static_group [vlan <vlan_name 32> vlanid <vidlist>] <ipaddr>
Description	<p>This command allows you to create an igmp snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group.</p> <p>The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.</p> <p>For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports.</p> <p>The static member port will only affect V2 IGMP operation.</p> <p>The Reserved IP multicast address 224.0.0.X must be excluded from the configured group. The VLAN must be created first before a static group can be created.</p>
Parameters	<p><vlan_name 32> – The name of the VLAN for which to create IGMP snooping static group information.</p> <p><vidlist> – The list of the VLAN IDs for which to create IGMP snooping static group information.</p> <p>< ipaddr > – The static group address for which to create IGMP snooping static group information. (for Layer 3 switch)</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a static group 226.1.1.1 for VID 1:

```
DES-3528:5#create igmp_snooping static_group vlanid 1 226.1.1.1
Command: create igmp_snooping static_group vlanid 1 226.1.1.1

Success.

DES-3528:5#
```

show igmp_snooping static_group

Purpose	Used to display a IGMP Snooping multicast group static member port.
Syntax	show igmp_snooping static_group {[vlan <vlan_name 32> vlanid <vidlist>] <ip6addr >}
Description	This command is used to display a IGMP Snooping multicast group static member port.
Parameters	<i>vlan</i> – The name of the VLAN on which the router port resides. <i>vlanid</i> – The ID of the VLAN on which the router port resides. <i>ipaddr</i> – Specifies the multicast group IP address. (for Layer 3 switch)
Restrictions	None.

Example usage

To display all the IGMP snooping static groups:

```
DES-3528:5#show igmp_snooping static_group
VLAN ID/Name          IP Address           Static Member Ports
-----
1 / Default           239.1.1.1           2:9-2:10

Total Entries : 1

DES-3528:5#
```

delete igmp_snooping static_group

Purpose	Used to delete the current IGMP snooping static group on the Switch.
Syntax	delete igmp_snooping static_group [vlan <vlan_name 32> vlanid <vidlist>] <ipaddr>
Description	This command is used to delete an igmp snooping static group and it will not affect the IGMP snooping dynamic member ports of a group.
Parameters	<vlan_name 32> – The name of the VLAN for which to delete IGMP snooping static group information. <vidlist> – The list of the VLAN IDs for which to delete IGMP snooping static group information. <ipaddr > – The static group address for which to delete IGMP snooping static group information. (for Layer 3 switch)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a static group 226.1.1.1 on VID 1:

```
DES-3528:5#delete igmp_snooping static_group vlanid 1 226.1.1.1
Command: delete igmp_snooping static_group vlanid 1 226.1.1.1

Success.

DES-3528:5#
```

config igmp_snooping static_group

Purpose	Used to configure the current IGMP snooping static group on the Switch.
Syntax	config igmp_snooping static_group [vlan <vlan_name 32> vlanid <vidlist>] <ipaddr> [add delete] <portlist>
Description	This command is used to add or delete a member port list of a specified static group.
Parameters	<p><vlan_name 32> – The name of the VLAN for which to configure IGMP snooping static group information.</p> <p><vidlist> – The list of the VLAN IDs for which to configure IGMP snooping static group information.</p> <p>< ipaddr > – The static group address for which to configure IGMP snooping static group information. (for Layer 3 switch)</p> <p>[add delete] <portlist> – Portlist to add or delete.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add port 5 to static group 226.1.1.1 on VID 1:

```
DES-3528:5#config igmp_snooping static_group vlanid 1 226.1.1.1 add 5
Command: config igmp_snooping static_group vlanid 1 226.1.1.1 add 5

Success.

DES-3528:5#
```

show igmp_snooping statistic counter

Purpose	Used to view the current IGMP snooping statistics on the Switch.
Syntax	show igmp_snooping statistic counter [vlan <vlan_name 32> vlanid <vidlist> ports <portlist>]
Description	This command is used to view this information, snooping must be enabled first.
Parameters	<p><vlan_name 32> – The name of the VLAN for which to view IGMP snooping statistic counter.</p> <p><vidlist> – The list of the VLAN IDs for which to view IGMP snooping statistic counter.</p> <p><portlist> – The list of the ports for which to view IGMP snooping statistic counter.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To view IGMP snooping statistic on VID 1:


```
DES-3528:5#show igmp_snooping statistic counter vlanid 1
```

```
Command: show igmp_snooping statistic counter vlanid 1
```

```
VLAN Name          : default
```

```
-----  
Group Number       : 1
```

```
Receive Statistics
```

```
Query
```

```
IGMP v1 Query      : 0  
IGMP v2 Query      : 0  
IGMP v3 Query      : 0  
Total              : 0  
Dropped By Rate Limitation : 0  
Dropped By Multicast VLAN : 0
```

```
Report & Leave
```

```
IGMP v1 Report     : 0  
IGMP v2 Report     : 0  
IGMP v3 Report     : 0  
IGMP v2 Leave      : 0  
Total              : 0  
Dropped By Rate Limitation : 0  
Dropped By Max Group Limitation : 0  
Dropped By Group Filter : 0  
Dropped By Multicast VLAN : 0
```

```
Transmit Statistics
```

```
Query
```

```
IGMP v1 Query      : 0  
IGMP v2 Query      : 0  
IGMP v3 Query      : 14  
Total              : 14
```

```
Report & Leave
```

```
IGMP v1 Report     : 0  
IGMP v2 Report     : 0  
IGMP v3 Report     : 0  
IGMP v2 Leave      : 0  
Total              : 0
```

```
Total Entries : 1
```

```
DES-3528:5#
```

clear igmp_snooping statistic counter

Purpose	Used to clear the current IGMP snooping statistic on the Switch.
Syntax	clear igmp_snooping statistic counter
Description	All IGMP snooping statistic counters will be cleared.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear IGMP snooping statistic counter:

```
DES-3528:5#clear igmp_snooping statistic counter
```

```
Command: clear igmp_snooping statistic counter
```

```
Success.
```

```
DES-3528:5#
```

config igmp_snooping data_driven_learning max_learned_entry

Purpose	Used to configure the max 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 the new data-driven groups. Traffic for the new groups will be dropped.
Parameters	<value 1-1024 > – The max number of groups that can be learned by data driven.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the max number of groups that can be learned by data driven:


```
DES-3528:5#config igmp_snooping data_driven_learning max_learned_
entry 100
```

```
Command: config igmp_snooping data_driven_learning max_learned_entry 100
```

```
Success.
```

```
DES-3528:5#
```

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 [all vlan_name <vlan_name> vlanid <vidlist>] { state [enable disable] aged_out [enable disable] expiry_time <sec 1-65535>}(1)
Description	<p>This command is used to configure the data driven learning of an IGMP snooping group.</p> <p>When data-driven learning is enabled for the VLAN, the switch receives the IP multicast traffic on this VLAN, and an IGMP snooping group will be created. The learning of an entry is not activated by IGMP membership registration, but by the multicast traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified so that it doesnt ageout or ageout by the aged timer.</p> <p>When data driven learning is enabled and data driven table is not full, the multicast filtering mode for all VLANs will be ignored. If the data driven learning table is full, the multicast traffic will be forwarded based on the setting of multicast filtering mode.</p>
	 <p>NOTE: If a data-driven group is created by the multicast traffic, and the same IGMP group joins from a member ports later, then the data-driven group will become an ordinary IGMP snooping group.</p>
Parameters	<p><i>vlan_name</i> <vlan_name> – The name of the VLAN for which IGMP snooping data driven learning is to be configured.</p> <p><i>vlanid</i> <vidlist> – The VID of the VLAN for which IGMP snooping data driven learning is to be configured.</p> <p><i>state</i> [enable disable] – Allows users to enable or disable IGMP snooping data driven learning for the specified VLAN.</p> <p><i>aged_out</i> [enable disable] – Allows users to enable or disable the aged_out time of the IGMP Snooping data driven learning for the specified VLAN.</p> <p><i>expiry_time</i> <second> – Allows users to set the time that an IGMP Snooping data driven learning group will expire for the specified VLAN.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable data driven learning on VLAN default:

```
DES-3528:5# config igmp_snooping data_driven_learning vlan_name default state enable
aged_out enable expiry_time 270
```

```
Command: config igmp_snooping data_driven_learning vlan_name default state enable
aged_out enable expiry_time 270
```

Success.

```
DES-3528:5#
```

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 [all [vlan_name <vlan_name> vlanid <vidlist>] [<ipaddr> all]]
Description	This command is used to delete the IGMP snooping group learned by data driven.
Parameters	<p><i>all</i> – Delete all groups learnt by data driven.</p> <p><i>vlan_name</i> <vlan_name 32> – The name of the VLAN for which IGMP snooping data driven learning group is to be deleted.</p> <p><i>vlanid</i> <vidlist> – The VID of the VLAN for which IGMP snooping data driven learning group is to be deleted.</p> <p><<i>ipaddr</i>> – The group address for which IGMP snooping data driven learning group is to be deleted on the specified VLAN.</p> <p><<i>all</i>> – All groups learnt by data driven on the specified VLAN will be deleted.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete all groups learnt by data driven on VLAN default:

```
DES-3528:5#clear igmp_snooping data_driven_group vlan_name default all
Command: clear igmp_snooping data_driven_group vlan_name default all

Success.

DES-3528:5#
```

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	<ipif_name 12> <ipaddr>
config dhcp_relay delete ipif	<ipif_name 12> <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 <desc 32>]
show dhcp_relay	{ipif <ipif_name 12>}
enable dhcp_relay	
disable dhcp_relay	
config dhcp_relay option_60 state	[enable disable]
config dhcp_relay option_60 add	string <mutiword 255> relay <ipaddr> [exact-match partial-match]
config dhcp_relay option_60 default	[relay <ipaddr> mode [relay drop]
config dhcp_relay option_60 delete	[string <mutiword 255> {relay <ipaddress>} ipaddress < ipaddr > all default {< ipaddr>}]
show dhcp_relay option_60	{[string <mutiword 255> ipaddress < ipaddr> default]}
config dhcp_relay option_61 state	[enable disable]
config dhcp_relay option_61 default	[relay <ipaddr> drop]
config dhcp_relay option_61 add	[mac_address <macaddr> string <desc_long 255>] [relay <ipaddr> drop]
config dhcp_relay option_61 delete	[mac_address <macaddr> string <desc_long 255> all]
show dhcp_relay option_61	
config dhcp_local_relay vlan	<vlan_name 32> 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_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	<p><i>hops</i> <value 1-16> – Specifies the maximum number of relay agent hops that the DHCP packets can cross.</p> <p><i>time</i> <sec 0-65535> – If this time is equal to or more than the entered value, the Switch will relay the DHCP packet.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config DHCP relay:

```
DES-3528:5#config dhcp_relay hops 2 time 23
Command: config dhcp_relay hops 2 time 23

Success.

DES-3528:5#
```

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 <ipif_name 12> <ipaddr>
Description	This command adds an IP address as a destination to forward (relay) DHCP/BOOTP relay packets to.
Parameters	<ipif_name 12> – The name of the IP interface in which DHCP relay is to be enabled. <ipaddr> – The DHCP server IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add an IP destination to the DHCP relay table:

```
DES-3528:5#config dhcp_relay add ipif System 10.58.44.6
Command: config dhcp_relay add ipif System 10.58.44.6

Success.

DES-3528:5#
```

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 <ipif_name 12> <ipaddr>
Description	This command is used to delete an IP destination addresses in the Switch's DHCP/BOOTP relay table.
Parameters	<ipif_name 12> – The name of the IP interface that contains the IP address below. <ipaddr> – The DHCP server IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IP destination from the DHCP relay table:

```
DES-3528:5#config dhcp_relay delete ipif System 10.58.44.6
Command: config dhcp_relay delete ipif System 10.58.44.6

Success.

DES-3528:5#
```

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><i>enable</i> – When this field is toggled to <i>Enabled</i> 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><i>disable</i> – If the field is toggled to <i>disable</i> 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 and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DES-3528:5#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DES-3528:5#
```

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><i>enable</i> – When the field is toggled to <i>enable</i>, 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><i>disable</i> – When the field is toggled to <i>disable</i>, the relay agent will not check the validity of the packet's option 82 field.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 check:

```
DES-3528:5#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DES-3528:5#
```

config dhcp_relay option_82 policy

Purpose	Used to configure the reforwarding policy of 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 reforwarding policy of DHCP relay agent information option 82 of the switch.
Parameters	<p><i>replace</i> – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>drop</i> – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>keep</i> – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 policy:

```
DES-3528:5#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DES-3528:5#
```

config dhcp_relay option_82 remote_id

Purpose	Used to configure the content in Remote ID suboption.
Syntax	config dhcp_relay option_82 remote_id [default user_define <desc 32>]
Description	This command is used to configure the content in Remote ID suboption.
Parameters	<p><i>default</i> – Uses the Switch's system MAC address as the remote ID.</p> <p><i>User_define <desc 32></i> – Uses user-defined string as the remote ID. Space is allowed in the string.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 remote ID:

```
DES-3528:5# config dhcp_relay option_82 remote_id user_define "D-Link L2 Switch"
Command: config dhcp_relay option_82 remote_id user_define "D-Link L2 Switch"

Success.

DES-3528:5#
```


show dhcp_relay

Purpose	Used to display the current DHCP/BOOTP relay configuration.
Syntax	show dhcp_relay {ipif <ipif_name 12>}
Description	This command will display the current DHCP relay configuration for the Switch, or if an IP interface name is specified, the DHCP relay configuration for that IP interface.
Parameters	<i>ipif <ipif_name 12></i> – 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-3528:5#show dhcp_relay
Command: show dhcp_relay

DHCP/Bootp Relay Status      : Disabled
DHCP/Bootp Hops Count Limit  : 4
DHCP/Bootp Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State : Disabled
DHCP Relay Agent Information Option 82 Check : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-21-91-AF-EA-00

Interface  Server 1      Server 2      Server 3      Server 4
-----
DES-3528:5#
```

Example usage:

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

```
DES-3528:5#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/Bootp Relay Status      : Disabled
DHCP/Bootp Hops Count Limit  : 4
DHCP/Bootp Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State : Disabled
DHCP Relay Agent Information Option 82 Check : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-21-91-AF-EA-00

Interface  Server 1      Server 2      Server 3      Server 4
-----
DES-3528:5#
```

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 and Operator-level users can issue this command.

Example usage:

To enable DHCP relay:

```
DES-3528:5#enable dhcp_relay
Command: enable dhcp_relay

Success.

DES-3528:5#
```

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.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable DHCP relay:

```
DES-3528:5#disable dhcp_relay
Command: disable dhcp_relay

Success.

DES-3528:5#
```

config dhcp_relay option_60 state

Purpose	This command is used to configure DHCP relay agent information option 60 state of the Switch. Used to config dhcp_relay option_60 state.
Syntax	config dhcp_relay option_60 state [enable disable]
Description	This command decides whether DHCP relay will process the DHCP option 60 or not. When enabled, if packets do not have option 60, then the relay servers cannot be determined based on option 60. Because the priority of option 60 and option 61 is higher than per IPIF configured servers, if the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored. If the relay servers are determined neither by option 60 nor option 61, then per IPIF configured servers will be used to determine the relay servers.
Parameters	<i>enable</i> – Enables the fuction. <i>disable</i> – Disables the fuction.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 60 state:

```
DES-3528:5#config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success.

DES-3528:5#
```

config dhcp_relay option_60 add

Purpose	This command is used to add a entry for dhcp_relay option_60
Syntax	config dhcp_relay option_60 add string <mutiword 255> relay <ipaddr> [exact-match partial-match]
Description	This command configures the option 60 relay rules. Note that different strings can be specified with the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.
Parameters	<i>exact-match</i> – The option 60 string in the packet must fully match the specified string. <i>partial-match</i> – The option 60 string in the packet only need partial match with the specified string. <i>string</i> – The specified string. <i>ipaddress</i> – Specify a relay server IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a new dhcp relay with option 60:

```
DES-3528:5#config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match
Command: config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match

Success.

DES-3528:5#
```

config dhcp_relay option_60 default

Purpose	This command is used to configure dhcp_relay option_60 default relay servers
Syntax	config dhcp_relay option_60 default [relay <ipaddr> mode[relay drop]]
Description	When there are no matching servers found for the DHCP client request packet based on option 60 string, the relay servers will be determined by the default relay server settings. On the other hand, if the drop option is specified, the packet with no matching rules found will be dropped without further actions. If the setting states relay, then the packet will be processed further based on option 61. The final relay servers will be the union of option 60 default relay servers and the relay servers determined by option 61.
Parameters	<i>ipaddress</i> – The specified ipaddress for dhcp_relay forward. Specifies a relay server IP for the packet that has mathcing option 60 rules. <i>drop</i> – Specify to drop the packet that has no matching option 60 rules. <i>relay</i> – The packet will be relayed based on the relay rules.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCP relay default option 60:

```
DES-3528:5#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

DES-3528:5#
```

config dhcp_relay option_60 delete

Purpose	This command is used to delete dhcp_relay option_60 entry.
Syntax	config dhcp_relay option_60 delete [string <mutiword 255> {relay <ipaddr>} ipaddress <ipaddr> all default {<ipaddr>}]
Description	This command can delete the entry specified by user. When all is specified, all rules excluding the default rules are deleted
Parameters	<p><i>string</i> – Deletes all the entries whose string is equal to the string specified if the IP address is not specified.</p> <p><i>relay <ipaddr></i> - Deletes one entry, whose string and IP address are equal to the string and IP address specified by the user.</p> <p><i>ipaddress</i> – Deletes any entry whose IP address is equal to the specified IP address.</p> <p><i>default</i> – Deletes any default relay IP address if ipaddress is not specified.</p> <p><i>Default<ipaddr></i> – Deletes all default relay ipaddress if IP address is not specified.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the DHCP relay option 60:

```
DES-3528:5#config dhcp_relay option_60 delete all
Command: config dhcp_relay option_60 delete all

Success.

DES-3528:5#
```

show dhcp_relay option_60

Purpose	This command is used to show dhcp_relay option_60 entry.
Syntax	show dhcp_relay option_60 [{string <mutiword 255> ipaddress <ipaddr> default}]
Description	This command will display the dhcp_relay option_60 entry by the user specified.
Parameters	<p><i>ipaddress</i> – Shows the entry whose ipaddress is equal to the specified ipaddress.</p> <p><i>default</i> – Shows the default behaviour of dhcp_relay option60.</p> <p><i>string</i> – Shows the entry whose string is equal to the string of a specified user.</p>
Restrictions	None.

Example usage:

To display the DHCP relay option 60:

```
DES-3528:5#show dhcp_relay option_60
Command: show dhcp_relay option_60

Default Processing Mode: Drop

Default Servers:

Matching Rules:

String          Match Type          IP Address
-----          -
abc             Exact Match         10.90.90.1

Total Entries : 1

DES-3528:5#
```

config dhcp_relay option_61 state

Purpose	This command is used to configure the DHCP relay option 61 state.
Syntax	config dhcp_relay option_61 state [enable disable]
Description	This command decides whether DHCP relay will process the DHCP option 61 or not. When enabled, if packets do not have option 61, then the relay servers cannot be determined based on option 61. Because the priority of option 60 and option 61 is higher than per IPIF configured servers, if the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored. If the relay servers are determined neither by option 60 nor option 61, then per IPIF configured servers will be used to determine the relay servers.
Parameters	<i>enable</i> – Enables the fuction dhcp_relay use option_61 ruler to relay dhcp packet. <i>disable</i> – Disables the fuction dhcp_relay use option_61 ruler to relay dhcp packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the state of DHCP relay option 61:

```
DES-3528:5#config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success.

DES-3528:5#
```

config dhcp_relay option_61 add

Purpose	This command is used to add a rule for dhcp_relay option_61.
Syntax	config dhcp_relay option_61 add [mac_address <macaddr> string <desc_long 255>] [relay <ipaddr> drop]
Description	This command adds a rule to determine the relay server based on option 61. The matched rule can be based on either the MAC address or a user-specified string. Only one relay server can be specified for a MAC-address or a string. Both option 60 and option 61 can assign particular DHCP relay sever, so they can altogether determine which relay server will be selected.
Parameters	<i>mac_address</i> – The client's client-ID which is the hardware address of client. <i>string</i> – The client's client-ID, which is specified by administrator. <i>relay</i> – Specify to relay the packet to a IP address. <i>drop</i> – Specify to drop the packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCP relay option 61:

```
DES-3528:5#config dhcp_relay option_61 add mac_address 00-01-22-33-44-55 drop
Command: config dhcp_relay option_61 add mac_address 00-01-22-33-44-55 drop

Success.

DES-3528:5#
```

config dhcp_relay option_61 default

Purpose	Used to determine the default action for option 61.
Syntax	config dhcp_relay option_61 default [relay <ipaddr> drop]
Description	This command is used to determine the rule to process those packets that have no option 61 matching rules. The default default-rule is drop.
Parameters	<i>relay</i> – Specifies to relay the packet that has no option 61 matching rules to an IP address. <i>drop</i> – Specifies to drop the packet that has no option 61 matching rules.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCP relay option 61 default:

```
DES-3528:5#config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success.

DES-3528:5#
```

config dhcp_relay option_61 delete

Purpose	This command is used to delete an option 61 rule.
Syntax	config dhcp_relay option_61 delete [mac_address <macaddr> string <desc_long 255> all]
Description	This command is used to delete an option 61 rule.
Parameters	<i>mac_address</i> – The entry with the specified MAC address will be deleted. <i>string</i> – The entry with the specified string will be deleted. <i>all</i> – All rules excluding the default rule will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the DHCP relay option 61 rules:

```
DES-3528:5#config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55
Command: config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55

Success

DES-3528:5#
```

show dhcp_relay option_61

Purpose	This command displays DHCP relay option 61.
Syntax	show dhcp_relay option_61
Description	This command displays DHCP relay option 61.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP relay option 61:

```
DES-3528:5#show dhcp_relay option_61
Command: show dhcp_relay option_61

Default Relay Rule:Drop

Matching Rules:

Client-ID                Type                Relay Rule
-----                -
00-01-22-33-44-55      MAC Address        Drop

Total Entries : 1

DES-3528:5#
```

config dhcp_local_relay vlan

Purpose	Used to enable or disable DHCP local relay function to the vlan.
Syntax	config dhcp_local_relay vlan <vlan_name 32> state [enable disable]
Description	This command is used to enable or disable the DHCP local relay function for a specified vlan. DHCP option 82 will also be automatically added.
Parameters	<vlan_name 32> – The name of the VLAN to be enabled by DHCP local relay. State – Enable or disable the DHCP local relay for a specified VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable DHCP local relay for the default VLAN:

```
DES-3528:5#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DES-3528:5#
```

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 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-3528:5#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DES-3528:5#
```

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 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-3528:5#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DES-3528:5#
```

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 local dhcp relay status:

```
DES-3528:5#show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status      : Disabled
DHCP/BOOTP Local Relay VID List    : 1

DES-3528:5#
```

802.1X COMMANDS (INCLUDING GUEST VLANs)

The Switch implements the server-side of the IEEE 802.1X Port-based and Host-based Network 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.

Command	Parameters
enable 802.1x	
disable 802.1x	
create 802.1x user	<username 15>
delete 802.1x user	<username 15>
show 802.1x user	
config 802.1x auth_protocol	[local radius_eap]
config 802.1x auth_failover	[enable disable]
config 802.1x fwd_pdu system	[enable disable]
config 802.1x fwd_pdu ports	[<portlist> all] [enable disable]
config 802.1x authorization network radius	[enable disable]
show 802.1x	{ [auth_state auth_configuration] ports {<portlist>} }
config 802.1x capability ports	[<portlist> all] [authenticator none]
config 802.1x max_users	[<value 1 – 448> no_limit]
config 802.1x auth_parameter ports	[<portlist> all] [default {direction [both in] port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> max_users [<value 1-448> no_limit] enable_reauth [enable disable]}(1)]
config 802.1x init	[port_based ports [<portlist> all>] mac_based ports [<portlist> all] {mac_address <macaddr>}]
config 802.1x 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>}]
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)
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	

Command	Parameters
show auth_statistics	{ports <portlist all>}
show auth_diagnostics	{ports <portlist all>}
show auth_session_statistics	{ports <portlist all>}
show auth_client	
show acct_client	
config accounting service	[network shell system] state [enable disable]
show accounting service	

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 enables the 802.1X Network Access control server 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 and Operator-level users can issue this command.

Example usage:

To enable 802.1X switch wide:

```
DES-3528:5#enable 802.1x
Command: enable 802.1x

Success.

DES-3528:5#
```

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 server 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 and Operator-level users can issue this command.

Example usage:

To disable 802.1X on the Switch:

```
DES-3528:5#disable 802.1x
Command: disable 802.1x

Success.

DES-3528:5#
```

create 802.1x user

Purpose	Used to create 802.1X user.
Syntax	create 802.1x user <username 15>
Description	This command creates a 802.1X user.
Parameters	<username 15> – Specifies adding user name
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create user “test”:

```
DES-3528:5#create 802.1x user test
Command: create 802.1x user test

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

Success.

DES-3528:5#
```

delete 802.1x user

Purpose	Used to delete 802.1X user.
Syntax	delete 802.1x user <username 15>
Description	This command deletes specified user.
Parameters	<username 15> – Specifies deleting user name
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete user “test”:

```
DES-3528:5#delete 802.1x user test
Command: delete 802.1x user test

Success.

DES-3528:5#
```

show 802.1x user

Purpose	Used to show 802.1X user.
Syntax	show 802.1x user
Description	This command displays the 802.1X user account information.
Parameters	None
Restrictions	None.

Example usage:

To display the 802.1X user information:

```
DES-3528:5#show 802.1x user
```

```
Command: show 802.1x user
```

```
Current Accounts:
```

```
Index           Username
-----
1               test
```

```
Total Entries:1
```

```
DES-3528:5#
```

config 802.1x auth_protocol

Purpose	Used to cofig the 802.1X auth protocol
Syntax	config 802.1x auth_protocol [local radius_eap]
Description	This command configures the 802.1X auth protocol.
Parameters	<i>local</i> – Specifies the auth protocol as local. <i>radius_eap</i> – Specifies the auth protocol as RADIUS EAP.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To config the 802.1X RADIUS EAP:

```
DES-3528:5#config 802.1x auth_protocol radius_eap
```

```
Command: config 802.1x auth_protocol radius_eap
```

```
Success.
```

```
DES-3528:5#
```

config 802.1x auth_failover

Purpose	Used to configure 802.1x auth_failover
Syntax	config 802.1x auth_failover [enable disable]
Description	When the authentication failover is disabled and Radius servers are unreachable, the authentication will fail. When the authentication failover is enabled and Radius servers authentication are unreachable, the local database will be used to do the authentication. The state is disabled by default.
Parameters	<i>enable</i> – Enables the authentication database fail over. <i>disable</i> – Disables the authentication database fail over.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config the 802.1X auth_failover:

```
DES-3528:5# config 802.1x auth_failover enable
```

```
Command: config 802.1x auth_failover enable
```

```
Success.
```

config 802.1x fwd_pdu system

Purpose	Used to configure the forwarding of EAPOL PDU when 802.1X is disabled.
Syntax	config 802.1x fwd_pdu system [enable disable]
Description	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports with 802.1X fwd_pdu enabled and 802.1X disabled (globally or just for the port). The default state is disable.
Parameters	None.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure forwarding of EAPOL PDU

```
DES-3528:5#config 802.1x fwd_pdu system enable
```

```
Command: config 802.1x fwd_pdu system enable
```

```
Success.
```

```
DES-3528:5#
```

config 802.1x authorization network

Purpose	Used to enable or disable the accepting of authorized configuration.
Syntax	config 802.1x authorization network radius [enable disable]
Description	This command is used to enable or disable the accepting of authorized configuration. When the authorization is enabled for 802.1x's radius, the authorized data assigned by the RADIUS server will be accepted by the Switch if the global authorization network is enabled.
Parameters	<i>radius</i> – When specified to enable, the authorization data assigned by the RADIUS server will be accepted by the Switch if the global authorization network is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable to accept the authorized data assigned from the RADIUS server.

```
DES-3528:5# config 802.1x authorization network radius disable
```

```
Command: config 802.1x authorization network radius disable
```

```
Success.
```

```
DES-3528:5#
```

config 802.1x fwd_pdu ports

Purpose	Used to configure if the port will flood EAPOL PDU when 802.1X functionality is disabled.
Syntax	config 802.1x fwd_pdu ports [<portlist> all] [enable disable]
Description	This is a per port setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports with 802.1X fwd_pdu enabled and 802.1X disabled (globally or just for the port). The default state is disable.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. <i>all</i> - Specifies all of ports to be displayed. <i>enable</i> - Enable flood EAPOL PDU on the ports. <i>disable</i> - Disable flood EAPOL PDU on the ports.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure 802.1X fwd PDU for ports:

```
DES-3528:5#config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu ports 1-2 enable

Success.
DES-3528:5#
```

show 802.1x

Purpose	Used to display the 802.1X state or configurations.
Syntax	show 802.1x { [auth_state auth_configuration] ports {<portlist>} }
Description	This command displays the 802.1X state or configurations.
Parameters	<i>auth_state</i> – Used to display 802.1X authentication state information of some ports. <i>auth_configuration</i> – Used to display 802.1X configurations of some ports. <i>portlist</i> – Specifies a range of ports to be displayed.
Restrictions	None.

Example usage:

To display the 802.1X states:

```

DES-3528:5# show 802.1x auth_state ports 1-3
Command: show 802.1x auth_state ports 1-3

Port   MAC Address           State           VLAN ID         Assigned
-----  -
1      00-00-00-00-00-01    Authenticated  4004            3
1      00-00-00-00-00-02    Authenticated  1234            -
1      00-00-00-00-00-04    Authenticating -                -
2      -                    (P) Authenticated 1234            -
3      -                    (P) Authenticating -                -

Total Authenticating Hosts :2
Total Authenticated Hosts  :3

DES-3528:5#

```

To display the 802.1X system level configurations:

```

DES-3528:5#show 802.1x
Command: show 802.1x

802.1X           : Enabled
Authentication Mode : Port_based
Authentication Protocol : Radius_EAP
Authentication Failover : Disabled
Forward EAPOL PDU   : Enabled
Max Users          : 448
RADIUS Authorization : Disabled

DES-3528:5#

```

To display the 802.1X configurations:


```
DES-3528:5#show 802.1x auth_configuration ports 1
```

```
Command: show 802.1x auth_configuration ports 1
```

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

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

config 802.1x capability

Purpose	Used to configure the port capability.
Syntax	config 802.1x capability ports [<portlist> all] [authenticator none]
Description	This command configures the port capability.
Parameters	<p><i>portlist</i> – Specifies a range of ports to be displayed.</p> <p><i>all</i> – Specifies all of ports to be displayed</p> <p><i>authenticator</i> – The port that wishes to enforce authentication before allowing access to services that are accessible via that Port adopts the authenticator role.</p> <p><i>none</i> – Allows the flow of PDUs via the Port</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port capability:

```
DES-3528:5#config 802.1x capability ports 1-10 authenticator
```

```
Command: config 802.1x capability ports 1-10 authenticator
```

```
Success.
```

```
DES-3528:5#
```

config 802.1x max _users

Purpose	Used to configure the max number of users that can be learned through 802.1x authentication.
Syntax	config 802.1x max users [<value 1 – 448> no_limit]
Description	The setting is a global limitation on the maximum number of users that can be learned through 802.1x authentication. In addition to the global limitation, per port max users is also limited. It is specified by config 802.1x auth_parameter command.
Parameters	<i>Max_users</i> – Specifies the maximum number of users. The number of the max users is 448 by default.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1x max users:

```
DES-3528:5# config 802.1x max users 200
Command: config 802.1x max users 200

Success.

DES-3528:5#
```

config 802.1x auth_parameter

Purpose	Used to configure the parameters that control the operation of the authenticator associated with a port.
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> max_users [<value 1-448> no_limit] enable_reauth [enable disable]}(1)]
Description	This command configures the parameters that control the operation of the authenticator associated with a port.
Parameters	<p><i>portlist</i> – Specifies a range of ports to be displayed.</p> <p><i>all</i> – Specifies all of ports to be displayed.</p> <p><i>default</i> – Sets all parameter to be default value.</p> <p><i>direction</i> – Sets the direction of access control .</p> <p style="padding-left: 40px;">both: For bidirectional access control.</p> <p style="padding-left: 40px;">in: For unidirectional access control.</p> <p><i>port_control</i> – You can force a specific port to be unconditionally authorized or unauthorized by setting the the parameter of port_control to be force_authorized or force_unauthorized. Besides, the controlled port will reflect the outcome of authentication if port_control is auto.</p> <p><i>quiet_period</i> – It is the initialization value of the quietWhile timer. The default value is 60 s and can be any value from 0 to 65535.</p> <p><i>tx_period</i> – It is the initialization value of the txWhen timer. The default value is 30 s and can be any value among 1 to 65535.</p> <p><i>supp_timeout</i> – The initialization value of the aWhile timer when timing out the supplicant. Its default value is 30 s and can be any value among 1 to 65535.</p> <p><i>server_timeout</i> – The initialization value of the aWhile timer when timing out the authentication server. Its default value is 30 and can be any value among 1 to 65535.</p> <p><i>max_req</i> – The maximum number of times that the authentication PAE state machine will retransmit an EAP Request packet to the supplicant. Its default value is 2 and can be any number among 1 to 10.</p> <p><i>reauth_period</i> – Its a nonzero number of seconds, which is used to be the re-authentication timer. The default value is 3600.</p> <p><i>max_users</i> - Specifies per port maximum number of users. The range is 1 to m. The default value is 16.</p> <p><i>enable_reauth</i> – You can enable or disable the re-authentication mechanism for a specific port.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DES-3528:5#config 802.1x auth_parameter ports 1-20 direction both
```

```
Command: config 802.1x auth_parameter ports 1-20 direction both
```

```
Success.
```

```
DES-3528:5#
```

config 802.1x auth_mode

Purpose	Used to configure 802.1X authentication mode.
Syntax	config 802.1x auth_mode [port_based mac_based]
Description	This command configures the authentication mode.
Parameters	<i>port_based</i> – Configure the authentication as Port-Based mode. <i>mac_based</i> – Configure the authentication as Host-Based mode.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the authentication mode:

```
DES-3528:5#config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DES-3528:5#
```

config 802.1x init

Purpose	Used to initialize the authentication state machine of some or all ports.
Syntax	config 802.1x init [port_based ports [<portlist all>] mac_based ports [<portlist> all] {mac_address <macaddr>}]
Description	This command used to initialize the authentication state machine of some or all.
Parameters	<i>port_based</i> – This instructs the Switch to init 802.1X functions based only on the port number. Ports approved for init can then be specified <i>mac_based</i> – This instructs the Switch to init 802.1X functions based only on the host address. MAC addresses approved for init can then be specified. <i>portlist</i> – Specifies a range of ports to be displayed. <i>all</i> – Specifies all of ports to be displayed. <i>mac_address</i> – Host address of client
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To initialize the authentication state machine of some or all:

```
DES-3528:5#config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-3528:5#
```

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><i>port_based</i> – 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><i>mac_based</i> – This instructs the Switch to re-authorize 802.1X functions based only on the host address. MAC addresses approved for re-authorization can then be specified.</p> <p><i>ports <portlist></i> – Specifies a port or range of ports to be re-authorized.</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>mac_address <macaddr></i> – Enter the MAC address to be re-authorized.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X reauthentication for ports 1 to 18:

```
DES-3528:5#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-3528:5#
```

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. 802.1X Guest 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 limited access rights on the Switch.
Parameters	<i><vlan_name 32></i> – 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	<p>Only Administrator and Operator-level users can issue this command.</p> <p>This VLAN must have already been previously created using the create vlan command.</p> <p>Only one VLAN can be set as the 802.1X Guest VLAN</p>

Example usage:

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

```
DES-3528:5#create 802.1x guest_vlan Trinity
Command: create 802.1x guest_vlan Trinity

Success.

DES-3528:5#
```

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]
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 and Operator-level users can issue this command.</p> <p>This VLAN must have already been previously created 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 original VLAN.</p>

Example usage:

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

```
DES-3528:5#config 802.1x guest_vlan ports 1-5 state enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DES-3528:5#
```

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. 802.1X Guest 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 limited access rights on the Switch.
Parameters	None.
Restrictions	This VLAN must have already been previously created using the create vlan command. Only one VLAN can be set as the 802.1X Guest VLAN.

Example usage:

To show 802.1X Guest VLAN.

```
DES-3528:5#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-----
Guest VLAN : Trinity
Enable Guest VLAN Ports: 5-8

Success.

DES-3528:5#
```

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. 802.1X Guest 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 limited access rights on the Switch.
Parameters	<vlan_name 32> – Enter the VLAN name of the 802.1X Guest VLAN to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command This VLAN must have already been previously created 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-3528:5#delete 802.1x guest_vlan Trinity
Command: delete 802.1x guest_vlan Trinity

Success.

DES-3528:5#
```

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 the auth_port, acct_port, timeout and retransmit parameters.</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 for a server reply. Default value is 5 seconds.</p> <p>retransmit <int 1-255> – The count for re-transmit. Default value is 2.</p>
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DES-3528:5#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-3528:5#
```

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	<i><server_index 1-3></i> – Assigns a number to the current set of RADIUS server settings. Up to 3 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-3528:5#config radius delete 1
Command: config radius delete 1

Success.

DES-3528:5#
```

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><i><server_index 1-3></i> – 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><i>ipaddress <server_ip></i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.</p> <ul style="list-style-type: none"> <i><passwd 32></i> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. <p><i>auth_port <udp_port_number 1-65535></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number 1-65535></i> – The UDP port number for accounting requests. The default is 1813.</p> <p><i>timeout <int 1-255></i> – The time in second for waiting for a server reply. Default value is 5 seconds.</p> <p><i>retransmit <int 1-255></i> – The count for re-transmit. Default value is 2.</p>
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DES-3528:5#config radius 1 ipaddress 10.48.74.121 key dlink_default
Command: config radius 1 ipaddress 10.48.74.121 key dlink_default

Success.

DES-3528:5#
```

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-3528:5#show radius
Command: show radius

Index  IP Address      Auth-Port  Acct-Port  Timeout  Retransmit  Key
-----  -
1      172.18.211.40   1812       1813       5        2           abc
2      172.18.211.71   1812       1813       5        2           123
3      172.18.211.108 1812       1813       5        2           lmn

Total Entries : 3

DES-3528:5#
```

show auth_statistics

Purpose	Used to display authenticator statistics information.
Syntax	show auth_statistics {ports <portlist> all}
Description	This command displays authenticator statistics information.
Parameters	<i>portlist</i> – Specifies a range of ports to be configured. <i>all</i> – All ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display authenticator statistics information from port 1:

```

DES-3528:5# show auth_statistics ports 1
Command: show auth_statistics ports 1

Port number : 1
EapolFramesRx           0
EapolFramesTx           6
EapolStartFramesRx      0
EapolReqIdFramesTx      6
EapolLogoffFramesRx     0
EapolReqFramesTx        0
EapolRespIdFramesRx     0
EapolRespFramesRx       0
InvalidEapolFramesRx    0
EapLengthErrorFramesRx  0
LastEapolFrameVersion   0
LastEapolFrameSource     00-00-00-00-00-00

DES-3528:5#

```

show auth_diagnostics

Purpose	Used to display authenticator diagnostics information
Syntax	show auth_diagnostics {ports <portlist> all}
Description	This command displays authenticator diagnostics information
Parameters	<i>portlist</i> – Specifies a range of ports to be configured. <i>all</i> – All ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display authenticator diagnostics information from port 1:

```

DES-3528:5#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port number : 1

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

DES-3528:5#

```

show auth_session_statistics

Purpose	Used to display authenticator session statistics information
Syntax	show auth_session_statistics {ports <portlist> all}
Description	This command displays authenticator session statistics information
Parameters	<i>portlist</i> – Specifies a range of ports to be configured. <i>all</i> – All port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display authenticator session statistics information from port 1:

```

DES-3528:5#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port number : 1

SessionOctetsRx           0
SessionOctetsTx           0
SessionFramesRx           0
SessionFramesTx           0
SessionId
SessionAuthenticMethod    Remote Authentication Server
SessionTime                0
SessionTerminateCause     SupplicantLogoff
SessionUserName
DES-3528:5#

```

show auth_client

Purpose	Used to display authentication client information
Syntax	show auth_client
Description	This command displays authentication client information
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display authentication client information:

```

DES-3528:5#show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses    0
radiusAuthClientIdentifier

radiusAuthServerEntry ==>
radiusAuthServerIndex :1

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

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

```

show acct_client

Purpose	Used to display account client information.
Syntax	show acct_client
Description	This command displays account client information
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display account client information:

```
DES-3528:5#show acct_client
```

```
Command: show acct_client
```

```
radiusAcctClient ==>
```

```
radiusAcctClientInvalidServerAddresses    0
```

```
radiusAcctClientIdentifier
```

```
radiusAuthServerEntry ==>
```

```
radiusAccServerIndex : 1
```

```
radiusAccServerAddress                    0.0.0.0
```

```
radiusAccClientServerPortNumber          0
```

```
radiusAccClientRoundTripTime             0
```

```
radiusAccClientRequests                  0
```

```
radiusAccClientRetransmissions           0
```

```
radiusAccClientResponses                 0
```

```
radiusAccClientMalformedResponses        0
```

```
radiusAccClientBadAuthenticators         0
```

```
radiusAccClientPendingRequests           0
```

```
radiusAccClientTimeouts                  0
```

```
radiusAccClientUnknownTypes              0
```

```
radiusAccClientPacketsDropped            0
```

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

config accounting service

Purpose	Used to configure the state of the specified RADIUS accounting service.
Syntax	config accounting service [network shell system] state [enable disable]
Description	This command is used to enable or disable the specified RADIUS accounting service.
Parameters	<p><i>network</i> – Accounting service for 802.1X port access control. By default, the service is disabled.</p> <p><i>shell</i> – Accounting service for shell events: When user login or logout the switch (via the console, Telnet, or SSH) and when timeout occurs, accounting information will be collected and sent to RADIUS server. By default, the service is disabled.</p> <p><i>system</i> – Accounting service for system events: reset, reboot. By default, the service is disabled.</p> <p><i>enable</i> – Enable the specified accounting service.</p> <p><i>disable</i> – Disable the specified accounting service.</p>
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure the accounting service:

```
DES-3528:5#config accounting service shell state enable
Command: config accounting service shell state enable

Success.

DES-3528:5#
```

show accounting service

Purpose	Used to show the RADIUS accounting services' status.
Syntax	show accounting service
Description	This command is used to show the state for radius accounting service.
Parameters	None
Restrictions	None.

Example usage:

To show accounting service:

```
DES-3528:5#show accounting service
Command: show accounting service

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

DES-3528:5#
```

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.

Access profiles allow establishment of a criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a VLAN-by-VLAN basis.

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 you want to deny all traffic to the subnet 10.42.73.0 to 10.42.73.255, you must first **create** an access profile that instructs the Switch to examine all of the relevant fields of each frame:

CREATE ACCESS_PROFILE PROFILE_ID 1 PROFILE_NAME 1 IP SOURCE_IP_MASK 255.255.255.0

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 identification number – in this case, **1**. 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. To restrict traffic, users must use the **deny** parameter.

Now that an access profile has been created, you must add the criteria the Switch will use to decide if a given frame should be forwarded or filtered. Here, we want to filter any packets that have an IP source address between 10.42.73.0 and 10.42.73.255:

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 1 deny

Here 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, you can assign an **access_id** that both identifies the rule and establishes a priority within the list of rules. A lower **access_id** gives the rule a higher priority. In case of a conflict in the rules entered for an access profile, the rule with the highest priority (lowest **access_id**) will take precedence.

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. Finally, 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.

Due to a chipset limitation, the Switch supports a maximum of 6 access profiles. The rules used to define the access profiles are limited to a total of 768 rules for the Switch. One rule can support ACL per port or per portmap.

The access profile 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 source_mac <macmask 000000000000-ffffffff> destination_mac <macmask 000000000000-ffffffff> 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_chunk_1 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) ipv6 [{ class flowlabel [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> }] } (1) source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask>]}(1)]profile_id <value 1-14> profile_name <name 1-32>
delete access_profile	[profile_id <value 1-14> all profile_name <name 1-32 >]

Command	Parameters
config access_profile	[profile_id <value 1-14> profile_name <name 1-32>] [add access_id [auto_assign <value 1-128>] [ethernet {[vlan <vlan_name 32> vlan_id <value 1-4094>] source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>}(1) ip{[vlan <vlan_name 32> vlan_id <value 1-4094>] source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> {user_define <hex 0x0-0xffff>}}(1) packet_content { offset_chunk_1 <hex 0x0-0xffff> offset_chunk_2 <hex 0x0-0xffff> offset_chunk_3 <hex 0x0-0xffff> offset_chunk_4 <hex 0x0-0xffff>}(1) ipv6 {[{ class <value 0-255> flowlabel <hex 0x0-0xffff> [tcp { src_port <value 0-65535> dst_port <value 0-65535> } udp { src_port <value 0-65535> dst_port <value 0-65535> }] } (1) source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr>}(1)] [port [<portlist> all] vlan_based [vlan_name <vlan_name> vlan_id <value 1-4094>]] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-15624>] [replace_dscp_with <value 0-63> replace_tos_precedence_with <value 0-7>] counter[enable disable]} mirror deny] {time_range <range_name 32>} delete access_id <value 1-128>]
show access_profile	{profile_id <value 1-14> profile_name <name 1-32 >}
enable cpu_interface_filtering	
disable cpu_interface_filtering	
create cpu access_profile	profile_id <value 1-5> [ethernet {vlan source_mac <macmask 000000000000-ffffffff > destination_mac <macmask 000000000000-ffffffff > 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 0x0-0xffff>}}(1) packet_content_mask {offset 0-15 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> offset 16-31 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> {offset 32-47 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> {offset 48-63 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> {offset 64-79 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff>}}(1) ipv6 { class flowlabel source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask> } (1)]
delete cpu access_profile	[profile_id <value 1-5 all]
config cpu access_profile profile_id	<value 1-5>[add access_id <value 1-100>[ethernet {[vlan <vlan_name 32> vlan_id <value 1-4094>] source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>}(1) ip{[vlan <vlan_name 32> vlan_id <value 1-4094>] source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> {user_define <hex 0x0-0xffff>}}(1) packet_content {offset_0-15 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> offset_16-31 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> offset_32-47 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> offset_48-63 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> offset_64-79 <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff> <hex 0x0-0xffff>}}(1) ipv6 {[{ class <value 0-255> flowlabel <hex 0x0-0xffff> } source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr>}(1)]port [<portlist> all][permit deny] {time_range <range_name 32>} delete access_id <value 1-100>]
show cpu access_profile	profile_id <value 1-5>

Command	Parameters
config flow_meter	[profile_id <value 1-14> profile_name <name 1-32>] access_id <value 1-128>[[tr_tcm cir <value 0-15624> {cbs <value 0-16384>} pir <value 0-15624> {pbs <value 0-16384>} sr_tcm cir <value 0-15624> cbs <value 0-16384> ebs <value 0-16384>] {conform permit {replace_dscp <value 0-63>} {counter [enable disable]}} exceed [permit {replace_dscp <value 0-63>} {counter [enable disable]} drop] violate [permit {replace_dscp <value 0-63>} {counter [enable disable]} drop] delete]
show flow_meter	{[profile_id <value 1-14> profile_name <name 1-32>] {access_id <value 1-128>}}
config time_range	<range_name 32> [hours start_time < time hh:mm:ss > end_time < time hh:mm:ss > weekdays <daylist> delete]
show time_range	
show current_config access_profile	

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 create access_profile command below.
Syntax	create access_profile [ethernet{ vlan source_mac <macmask 000000000000-ffffffff> destination_mac <macmask 000000000000-ffffffff> 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_chunk_1 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) ipv6 {{ class flowlabel [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>}]} (1) source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask>}(1)]profile_id <value 1-14> profile_name <name 1-32>
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><i>ethernet</i> – Specifies that the Switch will examine the layer 2 part of each packet header.</p> <ul style="list-style-type: none"> <i>vlan</i> – Specifies that the Switch will examine the VLAN part of each packet header. <i>source_mac <macmask 000000000000-ffffffff></i> – Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format. <i>destination_mac <macmask 000000000000-ffffffff></i> – Specifies a MAC address mask for the destination MAC address. <i>802.1p</i> – Specifies that the Switch will examine the 802.1p priority value in the frame's header. <i>ethernet_type</i> – Specifies that the Switch will examine the Ethernet type value in each frame's header.

create access_profile

ip – Specifies that the Switch will examine the IP address in each frame's header.

vlan – Specifies a VLAN mask.

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 frame's Transmission 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 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 User 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 <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.

packet_content_mask – Allows users to examine up to 4 specified *offset_chunk* within a packet at one time and specifies that the Switch will mask the packet header beginning with the *offset* value specified as follows:

packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff> }

With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), D-Link xStack switch family can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is the reason why Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

profile_id <value 1-14> – 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 1-14, yet, remember only 14 access profiles can be created on the Switch.

profile_name – Specifies the name of the profile. The maximum length is 32 characters.

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.

- *class* – Entering this parameter will instruct the Switch to examine the *class* field of the

create access_profile

IPv6 header. This class field is a part of the packet 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.
- *tcp* – Specifies that the Switch will examine each frame's Transmission 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.
- *udp* – Specifies that the Switch will examine each frame's User Datagram Protocol (UDP) 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.
- *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.

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

Example usage:

To create an access list rules:

```
DES-3528:5#create access_profile profile_id 5 profile_name 5 ethernet vlan source_mac
00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type
Command: create access_profile profile_id 5 profile_name 5 ethernet vlan source_mac
00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type

Success.

DES-3528:5#
```

delete access_profile

Purpose Used to delete a previously created access profile.

Syntax `delete access_profile [profile_id <value 1-14> | all | profile_name <name 1-32 >]`

Description This command is used to delete a previously created access profile on the Switch.

Parameters

- profile_id* <value 1-14> – Enter an integer between 1 and 14 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 14, yet, remember only 14 access profiles can be created on the Switch.
- profile_name* – Specifies the name of the profile. The maximum length is 32 characters.
- all* – Entering this parameter will delete all access profiles currently configured on the Switch.

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

Example usage:

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

```
DES-3528:5#delete access_profile profile_id 1
```

```
Command: delete access_profile profile_id 1
```

```
Success.
```

```
DES-3528:5#
```

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 1-14> profile_name <name 1-32>] [add access_id [auto_assign <value 1-128>][ethernet {[vlan <vlan_name 32> vlan_id <value 1-4094>] source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> 802.1p <value 0-7> ethernet_type <hex 0x0- 0xffff>}(1) ip{[vlan <vlan_name 32> vlan_id <value 1-4094>] source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> {user_define <hex 0x0-0xffff>}}](1) packet_content { offset_chunk_1 <hex 0x0-0xffff> offset_chunk_2 <hex 0x0- 0xffff> offset_chunk_3 <hex 0x0-0xffff> offset_chunk_4 <hex 0x0-0xffff>}(1) ipv6 [{ { class <value 0-255> flowlabel <hex 0x0-0xffff> [tcp { src_port <value 0- 65535> dst_port <value 0-65535> } udp { src_port <value 0-65535> dst_port <value 0-65535> } }] (1) source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr>}(1)] [port [<portlist> all] vlan_based [vlan_name <vlan_name> vlan_id <value 1-4094>] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-15624>] [replace_dscp_with <value 0-63> replace_tos_precedence_with <value 0-7>] counter[enable disable]] mirror deny] {time_range <range_name 32>} delete access_id <value 1-128>]</pre>
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	<p><i>profile_id</i> <value 1-14> – 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 14, yet, remember only 14 access profiles can be created on the Switch.</p> <p><i>profile_name</i> – Specifies the name of the profile. The maximum length is 32 characters.</p> <p><i>add access_id</i> <value 1-128> – 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.</p> <p><i>ethernet</i> – Specifies that the Switch will look only into the layer 2 part of each packet.</p> <p><i>vlan</i> <vlan_name 32> – Specifies that the access profile will only apply to this VLAN.</p> <p><i>vlan_id</i> <value 1-4094> - Specifies that the access profile will only apply to this VLAN ID.</p> <p><i>source_mac</i> <macaddr 000000000000-ffffffff> – Specifies that the access profile will apply to only packets with this source MAC address.</p> <p><i>destination_mac</i> <macaddr 000000000000-ffffffff> – Specifies that the access profile will apply to only packets with this destination MAC address.</p> <p><i>802.1p</i> <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.</p> <p><i>ethernet_type</i> <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>

config access_profile

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 this VLAN.

vlan_id <value 1-4094> - Specifies that the access profile will only apply to 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 <value 0-255> – Specifies that the access profile will apply to this ICMP type value.

code <value 0-255> – Specifies that the access profile will apply to this ICMP code value.

igmp – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

type <value 0-255> – Specifies that the access profile will apply to packets that have this IGMP type value.

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.

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 User 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.

user_define <hex 0x0-0xffffffff> – Specifies a mask to be combined with the value found in the frame header and if this field contains the value entered here, apply the following rules.

packet_content_mask – Allows users to examine any up to four specified offset_chunk within a packet at one time and specifies that the Switch will mask the packet header beginning with the offset value specified as follows:

packet_content { offset_chunk_1 <hex 0x0-0xffffffff> | offset_chunk_2 <hex 0x0-0xffffffff> | offset_chunk_3 <hex 0x0-0xffffffff> | offset_chunk_4 <hex 0x0-0xffffffff>

With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), D-Link xStack switch family can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is the reason that Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

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.

- *class* – Entering this parameter will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet 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

config access_profile

- *tcp* – Specifies that the Switch will examine each frame’s Transmission 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.
- *udp* – Specifies that the Switch will examine each frame’s User Datagram Protocol (UDP) 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.
- *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.

port <portlist> – Specifies the port number on the Switch to permit, deny or mirror access for the rule.

permit – Specifies the rule permit access for incoming packets on the previously specified port.

priority <value 0-7> – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header for incoming packets on the previously specified port.

{*replace_priority*} – Allows users to specify a new value to be written to the priority field of an incoming packet on the previously specified port.

replace_dscp_with <value 0-63> – Allows users to specify a new value to be written to the DSCP field of an incoming packet on the previously specified port.

replace_tos_precedence_with <value 0-7> – Specifies the packets that match the access profile and that tos-precedence values will be changed by the switch.

rx_rate – Specifies that one of the parameters below (*no_limit* or <value 1-15624>) will be applied to the rate at which the above specified ports will be allowed to receive packets

- *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports.
- <value 1-15624> – Specifies the packet limit, in 64Kbps, that the above ports will be allowed to receive.

deny – Specifies the rule will deny access for incoming packets on the previously specified port.

mirror – Specifies the packets that match the access profile, copies it and sends the copied one to the mirror port.

time_range – Specifies the time_range profile that has been associated with the ACL entries.

delete_access_id <value 1-128> – Use this to remove a previously created access rule of a profile ID. For information on number of rules that can be created for a given port, please see the introduction to this chapter.

Restrictions

Only Administrator and Operator-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-3528:5#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-3528:5#



NOTE: Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC Address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN (known as ARP spoofing attack). For a more detailed explanation on how ARP protocol works and how to employ D-Link's advanced unique Packet Content ACL to prevent an ARP spoofing attack, please see Appendix B, at the end of this manual.

show access_profile

Purpose	Used to display the currently configured access profiles on the Switch.
Syntax	show access_profile {profile_id <value 1-14> profile_name <name 1-32 >}
Description	This command is used to display the currently configured access profiles.
Parameters	<p><i>profile_id <value 1-14></i> – 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 14, yet, remember only 14 access profiles can be created on the Switch.</p> <p><i>profile_name <name 1-32 ></i> – Specifies the name of the profile. The maximum length is 32 characters.</p>
Restrictions	None.

Example usage:

To display all of the currently configured access profiles on the Switch:

```
DES-3528:5#show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries:1773
Total Used Rule Entries  :19

Access Profile ID: 5                Type : Ethernet
=====
Profile Name:5
Owner      : ACL
MASK Option :
VLAN      Source MAC      Destination MAC  802.1P  Ethernet Type
-----  -
          00-00-00-00-00-01  00-00-00-00-00-02
-----  -
=====
Unused Entries: 128

Access Profile ID: 13               Type : Ethernet IP
=====
Owner      : IGMP/MLD Snoop
MASK Option :
CTRL+C   ESC   q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

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 create cpu access_profile
----------------	--

create cpu access_profile

command, below.

Syntax

```
create cpu access_profile profile_id <value 1-5> [ethernet {vlan | source_mac
<macmask 000000000000-ffffffff > | destination_mac <macmask 000000000000-
ffffffff > | 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 **create cpu access_profile** command, below.

Parameters

- ethernet* – Specifies that the Switch will examine the layer 2 part of each packet header.
- *vlan* – Specifies that the Switch will examine the VLAN part of each packet header.
 - *source_mac <macmask 000000000000-ffffffff >* – Specifies to examine the source MAC address mask.
 - *destination_mac <macmask 000000000000-ffffffff >* – Specifies to examine the destination MAC address mask.
 - *802.1p* – Specifies that the Switch will examine the 802.1p priority value in the frame's header.
 - *ethernet_type* – Specifies that the Switch will examine the Ethernet type value in each frame's header.
- ip* – Specifies that the switch will examine the IP address in each frame's header.
- *vlan* – Specifies a VLAN mask.
 - *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 frame's Transmission 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 User Datagram Protocol

create cpu access_profile

Parameters	<p>(UDP) field.</p> <ul style="list-style-type: none"> • <i>src_port_mask</i> <hex 0x0-0xffff> – Specifies a UDP port mask for the source port. • <i>dst_port_mask</i> <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port. • <i>protocol_id_mask</i> <hex 0x0-0xffffffff> – Specifies that the Switch will examine each frame's Protocol ID field using the hex form entered here. • <i>user_define_mask</i> <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header. • <i>packet_content_mask</i> – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows: <ul style="list-style-type: none"> • <i>offset_0-15</i> – Enter a value in hex form to mask the packet from byte 0 to byte 15. • <i>offset_16-31</i> – Enter a value in hex form to mask the packet from byte 16 to byte 31. • <i>offset_32-47</i> – Enter a value in hex form to mask the packet from byte 32 to byte 47. • <i>offset_48-63</i> – Enter a value in hex form to mask the packet from byte 48 to byte 63. • <i>offset_64-79</i> – Enter a value in hex form to mask the packet from byte 64 to byte 79. <p><i>IPV6</i> – 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.</p> <ul style="list-style-type: none"> • <i>class</i> – Entering this parameter will instruct the Switch to examine the <i>class</i> field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4. • <i>flowlabel</i> – Entering this parameter will instruct the Switch to examine the <i>flow label</i> 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. • <i>source_ipv6_mask</i> <ipv6mask> – Specifies an IP address mask for the source IPv6 address. <p><i>destination_ipv6_mask</i> <ipv6mask> – Specifies an IP address mask for the destination IPv6 address.</p> <p><i>profile_id</i> <value 1-5> – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be created with this command.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a CPU access profile:

```
DES-3528:5#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-3528:5#
```

delete cpu access_profile

Purpose	Used to delete a previously created CPU access profile.
Syntax	delete cpu access_profile [profile_id <value 1-5 all>]
Description	This command is used to delete a previously created CPU access profile.
Parameters	<p><i>profile_id</i> <value 1-5> – Enter an integer between 1 and 5 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.</p> <p><i>all</i> – This will delete all previously configured cpu access_profiles.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DES-3528:5#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3528:5#
```

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	onfig cpu access_profile profile_id <value 1-5>[add access_id <value 1-100>[ethernet {[vlan <vlan_name 32> vlan_id <value 1-4094>] source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>}(1) ip {[vlan <vlan_name 32> vlan_id <value 1-4094>] source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp { type <value 0-255> code <value 0-255>} igmp { type <value 0-255>} tcp { src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin } udp { src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> { user_define <hex 0x0-0xffffffff>}]}(1) packet_content { offset_0-15 <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>} (1)] port [<portlist> all] [permit deny] [time_range <range_name 32>] delete access_id <value 1-100>]
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 config cpu access_profile command, above.
Parameters	<p><i>profile_id</i> <value 1-5> – 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 cpu 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> <p><i>add access_id</i> <value 1-100> – Adds an additional rule to the above specified access profile. The value is used to index the rule created.</p> <p><i>ethernet</i> – Specifies that the Switch will look only into the layer 2 part of each packet.</p> <p><i>vlan</i> <vlan_name 32> – Specifies that the access profile will only apply to this VLAN.</p> <p><i>vlan_id</i> <value 1-4094> - Specifies that the access profile will only apply to this VLAN ID.</p> <p><i>source_mac</i> <macaddr 000000000000-ffffffff> – Specifies that the access profile will apply to this source MAC address.</p> <p><i>destination_mac</i> <macaddr 000000000000-ffffffff> – Specifies that the access profile will apply to this destination MAC address.</p> <p><i>ethernet_type</i> <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><i>ip</i> – Specifies that the Switch will look into the IP fields in each packet.</p>

config cpu access_profile**Parameters**

vlan <vlan_name 32> – Specifies that the access profile will only apply to this VLAN.

vlan_id <value 1-4094> – Specifies that the access profile will only apply to 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* <value 0-255> – Specifies that the access profile will apply to this ICMP type value.
- *code* <value 0-255> – Specifies that the access profile will apply to this ICMP code value.

igmp – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

- *type* <value 0-255> – Specifies that the access profile will apply to packets that have this IGMP type value.

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.
- *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 urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize) and fin (finish).

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.

udp – Specifies that the Switch will examine the User Datagram Protocol (UDP) field within 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.

- *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

config cpu access_profile

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.

- *class* – Entering this parameter will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet 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.

permit | deny – Specifies that the packets forwarded to the CPU will either be permitted or denied based on the criteria defined in the CPU access profile.

time_range – Specifies the time range profile that has been associated with the ACL entries.

delete access_id <value 1-100> – Use this to remove a previously created access rule in a profile ID.

Restrictions

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

Example usage:

To configure CPU access list entry:

```
DES-3528:5#config cpu access_profile profile_id 5 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 deny
Command: config cpu access_profile profile_id 10 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 deny
Success.
DES-3528:5#
```

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 1-5>}
Description	This command is used view the current CPU interface filtering entries set on the Switch.
Parameters	<i>profile_id <value 1-5></i> – Enter an integer between 1 and 5 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-3528:5#show cpu access_profile
Command: show cpu access_profile
CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Total Unused Rule Entries:499
Total Used Rule Entries :1
```

```

Access Profile ID: 1                                     Type : IP
=====
MASK Option :
VLAN          Source IP Mask  Dst. IP Mask    DSCP ICMP Type Code
-----
                20.0.0.0      10.0.0.0
-----
-----

Access ID : 1                Mode: Deny
Ports: 1
-----
default        20.0.0.0        10.0.0.0        3                11        32

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

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 and Operator-level users can issue this command.

Example Usage:

To enable CPU interface filtering:

```

DES-3528:5#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3528:5#
    
```

disable cpu_interface_filtering

Purpose	Used to disable CPU interface filtering on the Switch.
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 and Operator-level users can issue this command.

Example Usage:

To disable CPU filtering:

```

DES-3528:5#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-3528:5#
    
```

config flow_meter

Purpose	Used to configure packet flow-based metering based on an access profile and rule.
----------------	---

config flow_meter

Syntax	<pre>config flow_meter [profile_id <value 1-14> profile_name <name 1-32>] access_id <value 1-128>[[tr_tcm cir <value 0-15624> {cbs <value 0-16384>} pir <value 0-15624> {pbs <value 0-16384>} sr_tcm cir <value 0-15624> cbs <value 0-16384> ebs <value 0- 16384>] {conform permit {replace_dscp <value 0-63>} {counter [enable disable]}} exceed [permit {replace_dscp <value 0-63>} {counter [enable disable]} drop] violate [permit {replace_dscp <value 0-63>} {counter [enable disable]} drop] [delete]</pre>
Description	<p>This command is used to configure the flow-based metering function. The metering function supports three modes, single rate two color, single rate three color, and two rate three color. The access rule must be created before the parameters in this command is configured.</p> <p>For the single rate two color mode, users may set the preferred bandwidth for this rule, in Kbps and once the bandwidth has been exceeded, overflow packets will be either dropped or set to a drop precedence, depending on the configuration. The drop precedence will be used by RED. With RED, the packet with higher drop precedence will be dropped with higher probability.</p> <p>For the single rate three color mode, users need to specify the committed rate in Kbps, the committed burst size and the excess burst size.</p> <p>For the two rate three color mode, users need to specify the committed rate in Kbps, the committed burst size, the peak rate and the peak burst size.</p> <p>The green color packet will be treated as the conforming action, the yellow color packet will be treated as the exceeding action, and the red color packet will be treated as the violating action.</p>
Parameters	<p><i>profile_id</i> <value 1-14> – 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 14.</p> <p><i>profile_name</i> <name 1-32> – Specifies the name of the profile. The maximum length is 32 characters.</p> <p><i>access_id</i> <value 1-128> – 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.</p> <p>replace_dscp: mark the packet with a specified DSCP. Different DSCP may have different probability to be dropped in the later stage.</p> <p><i>tr_tcm</i> – Specifies the “two rate three color mode”</p> <ul style="list-style-type: none"> cir <value 0-15624> – Specify the “committed information rate” The unit is 64Kbps. That is to say, 1 means 64Kbps. cbs <value 0-16384> – Specify the “committed burst size” <ol style="list-style-type: none"> 1. The unit is Kbyte. That is to say, 1 means 1Kbyte. 2. This parameter is an optional parameter. The default value is 4*1024. 3. The max set value is 16*1024. pir <value 0-15624> – Specify the “peak information rate” The unit is 64Kbps. That is to say, 1 means 64Kbps. pbs <value 0-16384> – Specify the “peak burst size” <ol style="list-style-type: none"> 1. The unit is Kbyte. That is to say, 1 means 1Kbyte. 2. This parameter is an optional parameter. The default value is 4*1024 3. The max set value is 16*1024. <p><i>sr_tcm</i> – Specifies the “single rate three color mode”</p> <ul style="list-style-type: none"> cir <value 0-15624> – Specify the “committed information rate” The unit is 64Kbps. That is to say, 1 means 64Kbps. cbs <value 0-16384> – Specify the “committed burst size” <ol style="list-style-type: none"> 1. The unit is Kbyte. That is to say, 1 means 1Kbyte. 2. The max set value is 16*1024.

config flow_meter

ebs <value 0-16384> – Specify the “excess burst size”

1. The unit is Kbyte. That is to say, 1 means 1 Kbyte.
2. The max set value is 16*1024.

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

permit – Permit the packet.

replace_dscp – Change the dscp of the packet.

counter – Specify the counter. This is optional. The default is “disable”.

exceed – Specifies the action when packet is in “yellow color”

permit – Permit the packet.

replace_dscp – Change the dscp of packet

drop – Drop the packet.

counter – Specify the counter. This is optional. The default is “disable”.

violate – Specifies the action when packet is in “red color”

Permit – Permit the packet.

replace_dscp – Change the dscp of packet.

counter – Specifies the counter. This is optional. The default is *disable*.

drop – Drop the packet.

The resource may be limited such that counter cannot be turned on. The counter will be cleared when the function is disabled.

delete – Delete the specified flow_meter.

Restrictions

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

Example usage:

To configure the ACL flow meter on the Switch:

```
DES-3528:5#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir 2000
pbs 2000 exceed permit replace_dscp 21 violate drop
```

```
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir 2000
pbs 2000 exceed permit replace_dscp 21 violate drop
```

Success.

```
DES-3528:5#
```

show flow_meter

Purpose Used to view the current state of ACL flow meter on the Switch.

Syntax **show flow_meter** {[profile_id <value 1-14> | profile_name <name 1-32>] {access_id <value1-128>}}

Description This command is used view the current state of ACL flow meter on the Switch.

Parameters

- profile_id* <value 1-14> – Specifies the profile ID.
- profile_name* <name 1-32> – Specifies the name of the profile. The maximum length is 32 characters.
- access_id* <value1-128> – Specifies the access ID.

Restrictions None.

Example usage:

To show the ACL flow meter state on the Switch:

```

DES-3528:5#show flow_meter
Command: show flow_meter

Flow Meter Information:
-----
Profile ID : 1      Access ID : 1      Mode : trTCM
CIR(64Kbps):1000   CBS(Kbyte):2000   PIR(64Kbps):2000   PBS(Kbyte):2000
Action:
    Conform : Permit      Replace DSCP : 11      Counter : Enabled
    Exceed  : Permit      Replace DSCP : 22      Counter : Enabled
    Violate : Drop        Counter : Disabled
-----

Profile ID : 1      Access ID : 2      Mode : srTCM
CIR(64Kbps):2500   CBS(Kbyte):2000   EBS(Kbyte):3500
Action:
    Conform : Permit      Replace DSCP:          Counter : Enabled
    Exceed  : Permit      Replace DSCP: 33      Counter : Enabled
    Violate : Drop        Counter : Disabled
-----

Total Entries: 2
DES-3528:5#
    
```

config time_range

Purpose	Used to configure the range of time to activate a function on the switch.
Syntax	config time_range <range_name 32> [hours start_time < time hh:mm:ss > end_time< time hh:mm:ss > weekdays <daylist> delete]
Description	This command defines a specific range of time to activate a function on the Switch by specifying which time range in a day and which days in a week are covered in the time range. Note that the specified time range is based on SNTP time or configured time. If this time is not available, then the time range will not be met.
Parameters	<p><i>range_name</i> – Specifies the name of the time range settings.</p> <p><i>start_time</i> – Specifies the starting time in a day. (24-hr time) For example, 19:00 means 7PM. 19 is also acceptable. start_time must be smaller than end_time.</p> <p><i>end_time</i> – Specifies the ending time in a day. (24-hr time)</p> <p><i>weekdays</i> – Specify the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days. For example, mon-fri (Monday to Friday) sun, mon, fri (Sunday, Monday and Friday)</p> <p><i>delete</i> – Deletes a time range profile. When a time_range profile has been associated with ACL entries, the delete of this time_range profile will fail.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config time range:

```
DES-3528:5#config time_range 1-3_new hours start_time 11:21:20 end_time 11:44:40
weekdays mon-fri
Command: config time_range 1-3_new hours start_time 11:21:20 end_time 11:44:40
weekdays mon-fri

Success.

DES-3528:5#
```

show time_range

Purpose	Used to display current access list table.
Syntax	show time_range
Description	This command displays current time range setting.
Parameters	None.
Restrictions	None.

Example usage:

To show the time range on the Switch:

```
DES-3528:5#show time_range
Command: show time_range

Time Range Information
-----
Range Name      : 1-3_new
Weekdays       : Mon,Tue,Wed,Thu,Fri
Start Time      : 11:21:20
End Time        : 11:44:40

Total Entries :1

DES-3528:5#
```

show current_config access_profile

Purpose	Used to display the ACL part of current configuration.
Syntax	show current_config access_profile
Description	This command displays the ACL privilege of the current configuration in user level of privilege. The overall current configuration can be displayed by show config command which is accessible in administrator level of privilege.
Parameters	None.
Restrictions	None.

Example usage:

To show the current configuration access profile on the Switch:

```
DES-3528:5#show current_config access_profile
Command: show current_config access_profile

#-----

# ACL

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

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

#-----

DES-3528:5#
```

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:

- a. It will limit bandwidth of receiving ARP packets.
- b. 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 CPU Interface Filtering mechanism 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. To keep the process moving fast, be sure not to add many conditions on which to accept these acceptable IP addresses and their packets, this limiting the CPU utilization.

Once in Exhausted mode, the packet flow will decrease by half of the level that caused the Switch to enter Exhausted mode. After the packet flow has stabilized, the rate will initially increase by 25% and then return to a normal packet flow.



NOTICE: When the Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

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>} 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	config safeguard_engine { state [enable disable] utilization { rising <value 20-100> falling <value 20-100>} 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><i>state [enable disable]</i> – Select the running state of the Safeguard Engine function as enable or disable.</p> <p><i>utilization</i> – Select this option to trigger the Safeguard Engine function to enable based on the following determinates:</p> <p><i>rising <value 20-100></i> – 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><i>falling <value 20-100></i> – 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><i>trap_log [enable disable]</i> – 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><i>mode [strict fuzzy]</i> – Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select:</p>

config safeguard_engine

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.

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 to all traffic flows.

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

Example usage:

To configure the safeguard engine for the Switch:

```
DES-3528:5#config safeguard_engine state enable utilization rising 45
Command: config safeguard_engine state enable utilization rising 45

Success.

DES-3528:5#
```

show safeguard_engine

Purpose	Used to display current Safeguard Engine settings.
Syntax	show safeguard_engine
Description	This will 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-3528:5#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     : Enabled
Mode                : Strict

DES-3528:5#
```

FILTER COMMANDS (DHCP SERVER/NETBIOS)

DHCP Server Screening Settings

This function allows you not only to restrict all DHCP Server packets but also to receive any specified DHCP server packets 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. It requires the support of ACL to enable the DHCP server filter function and it will create a deny rule with low priority to block the packets from the untrusted DHCP server. Similarly, the addition of a permitted DHCP entry should be created by ACL with high priority so as to permit packets from the trusted DHCP server.

When the DHCP Server filter function is enabled, all DHCP Server packets will be filtered from a specific port. Also, you are allowed to create entries for specific port-based Server IP address and Client MAC address binding entries. Be aware that the DHCP Server filter function must be enabled first. Once all settings are complete, all DHCP Server packets will be filtered from a specific port except those that meet the Server IP Address and Client MAC Address binding.

NetBIOS Filtering Setting

When the NetBIOS filter is enabled, all NetBIOS packets will be filtered from the specified port. Enabling the NetBIOS filter will create one access profile and create three access rules per port (UDP port numbers 137 and 138 and TCP port number 139).

For Extensive NetBIOS Filter, when it is enabled, all NetBIOS packets over 802.3 frames will be filtered from the specified port. This command is used to configure the state of the NetBIOS filter. Enabling the Extensive NetBIOS filter will create one access profile and create one access rule per port (DSAP (Destination Service Access Point) =F0, and SASP (Source Service Access Point) =F0).

The DHCP Server/NetBIOS Filter commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

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 netbios	[<portlist> all] state [enable disable]
show filter netbios	
config filter extensive_netbios	[<portlist> all] state [enable disable]
show filter extensive_netbios	

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

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	[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	<i>ipaddr</i> – The IP address of the DHCP server to be filtered <i>macaddr</i> – The MAC address of the DHCP client. <i>state</i> – Enable/Disable the DHCP filter state <i>ports <portlist></i> – The port number to which the DHCP filter will be applied.
Restrictions	Only Administrator-level users can issue this command. Enabling the DHCP filter will create one access profile and create one access rule per port (UDP port 67). Addition of a DHCP filter permit entry will create one access profile and create one access rule (DA = client MAC address, SA = source IP address and UDP port 67).

Example usage:

To add an entry from the DHCP server/client filter list in the switch's database:

```
DES-3528:5#config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-00-01 port 1-26
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-00-01 port 1-26

Success

DES-3528:5#
```

To configure the DHCP filter state:

```
DES-3528:5#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success

DES-3528:5#
```

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	Only Administrator users can issue this command.

Example usage:

To display the DHCP server filter list created on the switch:


```
DES-3528:5#show filter dhcp_server
Command: show filter dhcp_server

Filter DHCP Server Trap/Log State: Disabled
Illegal Server Log Suppress Duration:5 minutes
Enabled Ports: 1-3

Filter DHCP Server/Client Table
Server IP Address      Client MAC Address      Port
-----
10.255.255.254        00-00-00-00-00-01      1-28

Total Entries: 1

DES-3528:5#
```

config filter dhcp_server trap_log

Purpose	Used to enable or disable the trap or log that is triggered by the DHCP server filter events.
Syntax	config filter dhcp_server trap_log [enable disable]
Description	This command is used to enable or disable the trap or log that is triggered by the DHCP server filter events.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable log and trap for the DHCP server filter event.

```
DES-3528:5# config filter dhcp_server trap_log disable
Command: config filter dhcp_server trap_log disable

Success.

DES-3528:5#
```

config filter dhcp_server illegal_server_log_suppress_duration

Purpose	Used to configure the illegal server log suppress duration.
Syntax	config filter dhcp_server illegal_server_log_suppress_duration [1min 5min 30min]
Description	The DHCP server filtering function filters the illegal DHCP server packet. The DHCP server that sends the illegal packets will be logged. This command is used to suppress the logging of DHCP server that continues to send illegal DHCP packets. The same illegal DHCP server IP address detected will be logged only once within the duration.
Parameters	<i>illegal_server_log_suppress_duration [1min 5min 30min]</i> – if the same illegal DHCP server IP address is detected, it will be logged one time only within the duration. The log can be suppressed by one minute, 5 minutes or 30 minutes. The default value is 5 minutes.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the illegal_server_log_suppress_duration

```
DES-3528:5# config filter dhcp_server illegal _server_log_suppress_duration 30min
Command: config filter dhcp_server illegal _server_log_suppress_duration 30min

Success.

DES-3528:5#
```

config filter netbios

Purpose	Used to configure the switch to filter NetBIOS packets from specified ports.
Syntax	config filter netbios [<portlist> all] state [enable disable]
Description	This command will configure the switch to filter NetBIOS packets from the specified ports.
Parameters	<i><portlist></i> – The list of port numbers to which the NetBIOS filter will be applied. <i>state [enable disable]</i> – Used to enable/disable the NetBIOS filter on the switch.
Restrictions	Only Administrator-level users can issue this command. Enabling the NetBIOS filter will create one access profile and three access rules per port (UDP port number 137 and 138, and TCP port 139).

Example usage:

To configure the NetBIOS state:

```
DES-3528:5#config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

DES-3528:5#
```

show filter netbios

Purpose	Used to display the switch settings to filter NetBIOS packets from specified ports.
Syntax	show filter netbios
Description	This command will display the switch settings to filter NetBIOS packets from the specified ports.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the extensive NetBIOS filter status:

```
DES-3528:5#show filter netbios
Command: show filter netbios

Enabled Ports: 1-3

DES-3528:5#
```

config filter extensive_netbios

Purpose	Used to configure the switch to filter 802.3 frame NetBIOS packets from specified ports.
Syntax	config filter extensive_netbios [<portlist> all] state [enable disable]
Description	This command will configure the switch to filter 802.3 frame NetBIOS packets from the specified ports.
Parameters	<i><portlist></i> – The list of port numbers to which the NetBIOS filter will be applied. <i>state [enable disable]</i> – Used to enable/disable the NetBIOS filter on the switch.
Restrictions	Only Administrator-level users can issue this command. Enabling the NetBIOS filter will create one access profile and one access rules per port (DSAP=F0, SASP=F0).

Example usage:

To configure the extensive NetBIOS state::

```
DES-3528:5#config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

DES-3528:5#
```

show filter extensive_netbios

Purpose	Used to display the switch settings to filter NetBIOS packets from specified ports.
Syntax	show filter extensive_netbios
Description	This command will display the switch settings to filter NetBIOS packets from the specified ports.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the extensive NetBIOS filter status:

```
DES-3528:5#show filter extensive_netbios
Command: show filter extensive_netbios

Enabled Ports: 1-3

DES-3528:5#
```

L3 CPU FILTER COMMANDS

The L3 CPU Filter commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

When the Switch receives a packet such as PIM, DVMRP, OSPF, RIP, VRRP or IGMP query, the L3 CPU filter mode will determine how the packet is handled. If the mode is disabled, the packets will be sent to the CPU and will be treated according to the RFC standards. If the mode is enabled, the packets will be discarded. That means the packets will not be sent to the CPU and will not be propagated.

Command	Parameters
config cpu_filter l3_control_pkt	<portlist> [{dvmrp pim igmp_query}(1) all] state [enable disable]
show cpu_filter l3_control_pkt ports	{<portlist>}

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

config cpu_filter l3_control_pkt

Purpose	Used to discard the l3 control packets sent to CPU from specific ports.
Syntax	config cpu_filter l3_control_pkt <portlist> [{dvmrp pim igmp_query}(1) all] state [enable disable]
Description	This command is used to discard the l3 control packets sent to CPU from specific ports.
Parameters	<p><i>portlist</i> – Specifies the port list to filter control packet.</p> <p><i>dvmrp</i> – Specifies that the filtered L3 control protocol as DVMRP.</p> <p><i>pim</i> – Specifies that the filtered L3 control protocol as PIM.</p> <p><i>igmp_query</i> – Specifies that the filtered L3 control protocol as IGMP query.</p> <p><i>state</i> – Enable or disable the filtering function. Default is <i>disable</i>.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To filter DVMRP and PIM in port 1-26

```
DES-3528:5# config filter control_packet 1-26 dvmrp pim state enable
Command: config filter control_packet 1-26 dvmrp pim state enable

Success.

DES-3528:5#
```

show cpu_filter l3_control_pkt ports

Purpose	Used to display the l3 control packet CPU filtering status.
Syntax	show cpu_filter l3_control_pkt ports {<portlist>}
Description	This command is used to display the l3 control packet CPU filtering status.
Parameters	<i>portlist</i> – Specifies the port list to filter control packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the filtering status:

```
DES-3528:5# show cpu_filter l3_control_pkt ports 1:1-1:2
Command: show cpu_filter l3_control_pkt ports 1:1-1:2

Port      IGMP Query      DVMRP           PIM
-----  -
1:1      Disabled        Disabled        Disabled
1:2      Disabled        Disabled        Disabled

DES-3528:5#
```

LOOP-BACK DETECTION COMMANDS

The Loop-back 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 [value 0 <value 60-1000000>] interval <1-32767> mode [port-based vlan-based]} (1)
config loopdetect ports	[<portlist> all] state [enable disable]
config loopdetect trap	[none loop_detected loop_cleared both]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[all <portlist>]

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

config loopdetect

Purpose	Used to configure loop-back detection on the switch.
Syntax	config loopdetect {recover_timer [value 0 <value 60-1000000>] interval <1-32767> mode [port-based vlan-based]} (1)
Description	This command is used to configure loop-back detection on the switch.
Parameters	<p><i>recover_timer</i> – The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. The valid range is 60 to 1000000. Zero is a special value which means to disable the auto-recovery mechanism. The default value is 60.</p> <p><i>interval</i> – The time interval (inseconds) at which the remote device transmits all the CTP packets to detect the loop-back event. The default value is 10, with a valid range of 1 to 32767,</p> <p><i>mode</i> – In port-based mode, the port will be disabled during the loop detection. In vlan-based mode, the port cannot process VLAN packets destined for ports involved in detecting the loop.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the recover time to 0, and interval to 20, and VLAN-based mode:

```
DES-3528:5#config loopdetect recover_timer 0 interval 20 mode vlan-based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based
```

Success

```
DES-3528:5#
```

config loopdetect ports

Purpose	Used to configure loop-back detection on the switch.
Syntax	config loopdetect ports [<portlist> all] state [enable disable]
Description	This command is used to configure loop-back detection on the switch.
Parameters	<i><portlist></i> – Specifies a range of ports for the loop-back detection <i>state [enable disable]</i> – Allows the loop-back detection to be disabled and enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the loop-detect state to enable:

```
DES-3528:5#config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success

DES-3528:5#
```

config loopdetect trap

Purpose	Used to configure trap modes.
Syntax	config loopdetect trap [none loop_detected loop_cleared both]
Description	This command is used to configure trap modes.
Parameters	<i>none</i> – Trap will not be sent for both cases. <i>loop_detected</i> – Trap is sent when the loop condition is detected. <i>loop_cleared</i> – Trap is sent when the loop condition is cleared. <i>both</i> – Trap will be sent in both cases.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config loop trap both:

```
DES-3528:5#config loopdetect trap both
Command: config loopdetect trap both

Success.

DES-3528:5#
```

enable loopdetect

Purpose	Used to globally enable loop-back detection on the switch.
Syntax	enable loopdetect
Description	This command is used to globally enable loop-back detection on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable loop-back detection on the switch:

```
DES-3528:5#enable loopdetect
Command: enable loopdetect

Success

DES-3528:5#
```

disable loopdetect

Purpose	Used to globally disable loop-back detection on the switch.
Syntax	disable loopdetect
Description	This command is used to globally disable loop-back detection on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable loop-back detection on the switch:

```
DES-3528:5#disable loopdetect
Command: disable loopdetect

Success

DES-3528:5#
```

show loopdetect

Purpose	Used to display the current loop-back detection settings on the switch.
Syntax	show loopdetect
Description	This command is used to display the current loop-back detection settings on the switch
Parameters	None.
Restrictions	None.

Example usage:

To show loop-detect:

```
DES-3528:5#show loopdetect
Command: show loopdetect

LBD Global Settings
-----
LBD Status       : Disabled
LBD Mode         : Port-Based
LBD Interval     : 20
LBD Recover Time : 60
LBD Trap Status  : None

DES-3528:5#
```


show loopdetect ports

Purpose	Used to display the current per-port loop-back detection settings on the switch.
Syntax	show loopdetect ports [all <portlist>]
Description	This command is used to display the current per-port loop-back detection settings on the switch
Parameters	<portlist> – Specifies a range of ports for the loop-back detection all – Specifies all ports for the loop-back detection.
Restrictions	None.

Example usage:

To show loop-detect ports:

```
DES-3528:5#show loopdetect ports 1-3
Command: show loopdetect ports 1-3

Port  Loopdetect State  Loop Status
1      Enabled             Normal
2      Enabled             Loop!
3      Enabled             Normal

DES-3528:5#
```

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.

Command	Parameters
config traffic_segmentation	[<portlist> all] forward_list [null all <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> all] forward_list [null all <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>all – Specifies all the 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> <ul style="list-style-type: none"> • null – No ports are specified. • all – All ports are specified. • <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).
Restrictions	Only Administrator and Operator-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-3528:5#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15
Success.
DES-3528:5#
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the Switch.
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 forwarding list must be on the same Switch.

Example usage:

To display the current traffic segmentation configuration on the Switch.

```
DES-3528:5#show traffic_segmentation
```

```
Command: show traffic_segmentation
```

```
Traffic Segmentation Table
```

Port	Forward Portlist
1	1-26
2	1-26
3	1-26
4	1-26
5	1-26
6	1-26
7	1-26
8	1-26
9	1-26
10	1-26
11	1-26
12	1-26
13	1-26
14	1-26
15	1-26
16	1-26
17	1-26
18	1-26

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

sFLOW COMMANDS

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

Command	Parameters
enable sflow	
disable sflow	
show sflow	
create sflow flow_sampler	ports [<portlist> all] analyzer_server_id < value 1-4> { rate <value 0- 65535> maxheadersize < value 18-256>}
config sflow flow_sampler	ports [<portlist> all] { rate <value 0- 65535> maxheadersize < value 18-256>}(1)
delete sflow flow_sampler	ports [<portlist> all]
show sflow flow_sampler	
create sflow counter_poller	ports [<portlist> all] analyzer_server_id < value 1-4> {interval [disable <sec 20-120>]}
config sflow counter_poller	ports [<portlist> all] interval [disable <sec 20-120>]
delete sflow counter_poller	ports [<portlist> all]
show sflow counter_poller	
create sflow analyzer_server	< value 1-4 > owner<name 16> { timeout [<sec 1-2000000> infinite] collectoraddress <ipaddr> collectorport <udp_port_number 1-65535> maxdatagramsize < value 300-1400> }
config sflow analyzer_server	< value 1-4 > { timeout [<sec 1-2000000> infinite] collectoraddress <ipaddr> collectorport <udp_port_number 1-65535> maxdatagramsize < value 300-1400> }(1)
delete sflow analyzer_server	< value 1-4 >
show sflow analyzer_server	

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

enable sflow

Purpose	Used to enable the sFlow function.
Syntax	enable sflow
Description	This command enables the sFlow function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable sflow:

```
DES-3528:5#enable sflow
Command: enable sflow

Success.

DES-3528:5#
```

disable sflow

Purpose	Used to disable the sFlow function.
Syntax	disable sflow
Description	This command disables the sFlow function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable sflow:

```
DES-3528:5#disable sflow
Command: disable sflow

Success.

DES-3528:5#
```

show sflow

Purpose	Used to display the sFlow function.
Syntax	show sflow
Description	This command displays the sFlow function settings on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display sflow:

```
DES-3528:5#show sflow
Command: show sflow

sFlow Version   : 1.00
sFlow Address   : 10.24.73.21
sFlow State     : Disabled

DES-3528:5#
```

create sflow flow_sampler

Purpose	Used to create the sflow flow_sampler.
Syntax	create sflow flow_sampler ports [<portlist> all] analyzer_server_id < value 1-4> { rate <value 0- 65535> maxheadersize < value 18-256>}
Description	This command is used to create the sFlow flow_sampler. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to the analyzer server at the specified interval.
Parameters	<p><i>ports</i> – Specifies the list of ports to be configured.</p> <p><i>analyzer_server_id</i> – The analyzer_server_id specifies the ID of a server analyzer where the packet will be forwarded.</p> <p><i>rate</i> – The sampling rate for packet sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. As a result, one packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.</p> <p><i>maxheadersize</i> – The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create sflow flow_sampler:

```
DES-3528:5#create sflow flow_sampler ports all analyzer_server_id 1 rate 10
maxheadersize 100
```

```
Command: create sflow flow_sampler ports all analyzer_server_id 1 rate 10
maxheadersize 100
```

Success.

```
DES-3528:5#
```

config sflow flow_sampler

Purpose	Used to configure the sflow flow_sampler parameters.
Syntax	config sflow flow_sampler ports [<portlist> all] { rate <value 0- 65535> maxheadersize < value 18-256>}(1)
Description	This command configures the sflow flow_sampler parameters. If the user wants to change the analyzer_server_id, he needs to delete the flow_sampler and creates a new one.
Parameters	<p><i>ports</i> – Specifies the list of ports to be configured.</p> <p><i>rate</i> – The sampling rate for packet sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate is 5120. As a result, one packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.</p> <p><i>maxheadersize</i> – The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure sflow flow_sampler:

```
DES-3528:5#config sflow flow_sampler ports all rate 10 maxheadersize 100
Command: config sflow flow_sampler ports all rate 10 maxheadersize 100

Success.

DES-3528:5#
```

delete sflow flow_sampler

Purpose	Used to delete the sflow flow_sampler.
Syntax	delete sflow flow_sampler ports [<portlist> all]
Description	This command is used to delete the sflow flow_sampler that has been configured for the specified port.
Parameters	<i>ports</i> – Specifies the list of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete all the sflow flow_sampler:

```
DES-3528:5#delete sflow flow_sampler ports all
Command: delete sflow flow_sampler ports all

Success.

DES-3528:5#
```

show sflow flow_sampler

Purpose	Used to show the sflow flow_sampler information of ports which have been created.
Syntax	show sflow flow_sampler
Description	This command is used to show the sFlow flow_sampler which has been configured for ports. The actual value rate is 256 times the displayed rate value. There are two types of rates. ConfigRate is configed by the user. In order to limit the number of packets sent to the CPU when the rate of traffic to the CPU is high, the sampling rate will be decreased. This is specified as the active rate.
Parameters	None.
Restrictions	None.

Example usage:

To show the sflow flow_sampler:

```
DES-3528:5#show sflow flow_sampler
Command: show sflow flow_sampler
```

Port	Analyzer Server ID	Configured Rate	Active Rate	Max Header Size
----	-----	-----	-----	-----
1	1	20	80	140
2	2	10	40	100

```
Total Entries: 2

DES-3528:5#
```

create sflow counter_poller

Purpose	Used to create the counter poller for the sFlow function of the Switch.
Syntax	create sflow counter_poller ports [<portlist> all] analyzer_server_id <value 1-4> {interval [disable <sec 20-120>]}
Description	This command is used to configure the settings for the Switch's counter poller. This mechanism will take a poll of the IF counters of the Switch and package them with the other previously mentioned data into a datagram which will be sent to the sFlow Analyzer Server for examination.
Parameters	<i>ports</i> – Specifies the list of ports to be configured. <i>analyzer_server_id</i> – The analyzer_server_id is the id of a analyzer_server. <i>interval</i> – Users may configure the Polling Interval here. The Switch will take a poll of the IF counters every time this interval reaches 0, and this information will be included in the sFlow datagrams that will be sent to the sFlow Analyzer for examination. Choosing the disabled parameter will disable the counter polling for this entry. If interval is not specified, its default value is disable.
Restrictions	Only Administrators and Operator-level users can issue this command.

Example usage:

To create the sflow counter_poller:

```
DES-3528:5#create sflow counter_poller ports 1 analyzer_server_id 2 interval 40
Command: create sflow counter_poller ports 1 analyzer_server_id 2 interval 40

Success.

DES-3528:5#
```

config sflow counter_poller

Purpose	Used to configure the sflow counter_poller parameters.
Syntax	config sflow counter_poller ports [<portlist> all] interval [disable <sec 20-120>]
Description	This command is used to config the sflow counter_poller parameters. If the user wants the change the analyzer_server_id, he needs to delete the counter_poller and create a new one.
Parameters	<i>ports</i> – Specifies the list of ports to be configured. <i>interval</i> – The maximum number of seconds between successive statistic counter information. If set to disable, the counter-poller is disabled. If an interval is not specified, its default value is disable.
Restrictions	Only Administrators and Operator-level users can issue this command.

Example usage:

To configure the sflow counter_poller:


```
DES-3528:5#config sflow counter_poller ports 1 interval 40
Command: config sflow counter_poller ports 1 interval 40

Success.

DES-3528:5#
```

delete sflow counter_poller

Purpose	Used to delete the sflow counter_poller.
Syntax	delete sflow counter_poller ports [<portlist> all]
Description	This command deletes the sflow counter_poller from the specified port .
Parameters	<i>ports</i> – Specifies the list of ports to be configured.
Restrictions	Only Administrators and Operator-level users can issue this command.

Example usage:

To delete the sflow counter_poller:

```
DES-3528:5#delete sflow counter_poller ports 1
Command: delete sflow counter_poller ports 1

Success.

DES-3528:5#
```

show sflow counter_poller

Purpose	Used to show the sflow counter_poller information of ports which have been created.
Syntax	show sflow counter_poller
Description	This command is used to show the sflow counter_pollers which have been configured for port.
Parameters	None.
Restrictions	None.

Example usage:

To show the sflow counter_poller:

```
DES-3528:5#show sflow counter_poller
Command: show sflow counter_poller

Port      Analyzer Server ID      Polling Interval (secs)
-----  -
1          1                      25
2          3                      30

Total Entries: 2

DES-3528:5#
```

create sflow analyzer_server

Purpose	Used to create the analyzer_server.
Syntax	create sflow analyzer_server < value 1-4 > owner<name 16> { timeout [<sec 1-2000000> infinite] collectoraddress <ipaddr> collectorport <udp_port_number 1-65535> maxdatagramsize < value 300-1400> }
Description	This command creates the analyzer_server. You can specify more than one analyzer_server with the same IP address but with different UDP port numbers. You can have up to four unique combinations of IP addresses and UDP port numbers.
Parameters	<p><i>owner</i> – The entity making use of this sflow analyzer_server. When owner is set or modified, the timeout value will become 400 automatically.</p> <p><i>timeout</i> – The length of time before the server is timed out. When the analyzer_server times out, all of the flow_samplers and counter_pollers associated with this analyzer_server will be deleted. “infinite” indicates that analyzer_server never times out. If not specified, its default value is 400.</p> <p><i>collectoraddress</i> – The IP address of the analyzer_server. If not specified, the address will be 0.0.0.0 which means that the entry will be inactive.</p> <p><i>collectorport</i> – The destination UDP port for sending the sFlow datagrams. If not specified, the default value is 6364.</p> <p><i>maxdatagramsize</i> – The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the sflow analyzer_server:

```
DES-3528:5#create sflow analyzer_server 1 owner monitor
Command: create sflow analyzer_server 1 owner monitor

Success.

DES-3528:5#
```

config sflow analyzer_server

Purpose	Used to configure the analyzer_server information .
Syntax	config sflow analyzer_server < value 1-4 > { timeout [<sec 1-2000000> infinte] collectoraddress <ipaddr> collectorport <udp_port_number 1-65535> maxdatagramsize < value 300-1400> }(1)
Description	This command configures the receiver information. You can specify more than one collector with the same IP address if the UDP port numbers are unique.
Parameters	<p><i>timeout</i> – The length of time before the server is timed out. When the analyzer_server times out, all of the flow_samplers and counter_pollers associated with this analyzer_server will be deleted. “infinite” indicates that analyzer_server never times out. If not specified, its default value is 400.</p> <p><i>collectoraddress</i> – The IP address of the analyzer_server. If not specified, the address will be 0.0.0.0 which means that the entry will be inactive.</p> <p><i>collectorport</i> – The destination UDP port for sending the sFlow datagrams. If not specified, the default value is 6364.</p> <p><i>maxdatagramsize</i> – The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the sflow analyzer_server:

```
DES-3528:5#config sflow analyzer_server 2 collectoraddress 10.90.90.9
Command: config sflow analyzer_server 2 collectoraddress 10.90.90.9

Success.

DES-3528:5#
```

delete sflow analyzer_server

Purpose	Used to delete the analyzer_server.
Syntax	delete sflow analyzer_server < value 1-4 >
Description	This command deletes the analyzer_server.
Parameters	<i>value</i> – analyzer_server ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the sflow analyzer_server:

```
DES-3528:5#delete sflow analyzer_server 2
Command: delete sflow analyzer_server 2

Success.

DES-3528:5#
```

show sflow analyzer_server

Purpose	Used to show the sflow analyzer_server information.
Syntax	show sflow analyzer_server
Description	This command is used to show the sflow analyzer_server information. The Timeout field specifies the time configured by user. The Current countdown times is the current time remaining before the server timesout.
Parameters	None.
Restrictions	None.

Example usage:

To show the sflow analyzer_server:

```
DES-3528:5#show sflow analyzer_server
```

```
Command: show sflow analyzer_server
```

```
sFlow Analyzer_server Information
```

```
-----
```

```
Server ID           : 1  
Owner               : monitor  
Timeout             : 400  
Current Countdown Time: 400  
Collector Address   : 10.90.90.1  
Collector Port      : 6343  
Max Datagram Size  : 1400
```

```
Total Entries: 1
```

```
DES-3528:5#
```

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 ddmmyyyy > <time hh:mm:ss >
config time_zone	{operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>}
config dst	[disable repeating {s_week <start_week 1-4,last> s_day <start_day sun-sat> s_mth <start_mth 1-12> s_time <start_time hh:mm> e_week <end_week 1-4,last> e_day <end_day sun-sat> e_mth <end_mth 1-12> e_time <end_time hh:mm> offset [30 60 90 120]} annual {s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time hh:mm> e_date <end_date 1-31> e_mth <end_mth 1-12> e_time <end_time hh:mm> offset [30 60 90 120]}]
show time	

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><i>primary</i> – This is the primary server from which the SNTP information will be taken.</p> <p><i><ipaddr></i> – The IP address of the primary server.</p> <p><i>secondary</i> – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <p><i><ipaddr></i> – The IP address for the secondary server.</p> <p><i>poll-interval <int 30-99999></i> – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.</p>
Restrictions	Only Administrator and Operator-level users can issue this command. SNTP service must be enabled for this command to function (<i>enable sntp</i>).

Example usage:

To configure SNTP settings:

```
DES-3528:5#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-3528:5#
```

show sntp

Purpose	Used to display the SNTP information.
Syntax	show sntp
Description	This command will 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-3528:5#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-3528:5#
```

enable sntp

Purpose	Used to enable SNTP server support.
Syntax	enable sntp
Description	This command enables 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 and Operator-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-3528:5#enable sntp
Command: enable sntp

Success.

DES-3528:5#
```

disable sntp

Purpose	Used to disable SNTP server support.
Syntax	disable sntp
Description	This command disables SNTP support. SNTP service must be separately configured (see config sntp).
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable SNTP support:

```
DES-3528:5#disable sntp
Command: disable sntp

Success.

DES-3528:5#
```

config time

Purpose	Used to manually configure system time and date settings.
Syntax	config time <date ddmmmyyyy> <time hh:mm:ss>
Description	This command configures the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<p><i>date</i> – 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><i>time</i> – 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 and Operator-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-3528:5#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3528:5#
```

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 adjusts system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	<p><i>operator</i> – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT.</p> <p><i>hour</i> – Select the number of hours different from GMT.</p> <p><i>min</i> – Select the number of minutes difference added or subtracted to adjust the time zone.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DES-3528:5#config time_zone operator + hour 2 min 30
```

```
Command: config time_zone operator + hour 2 min 30
```

```
Success.
```

```
DES-3528:5#
```

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 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]`

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.

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 1-4,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 1-4,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.

config dst

- 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 and Operator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DES-3528:5#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-3528:5#
```

show time

Purpose	Used to display the current time settings and status.
Syntax	show time
Description	This command displays system time and date configuration as well as display current system time.
Parameters	None.
Restrictions	None.

Example usage:

To show the time currently set on the Switch's System clock:

```
DES-3528:5#show time
Command: show time

Current Time Source   : System Clock
Boot Time             : 11 Mar 2000 17:41:32
Current Time         : 11 Mar 2000 22:10:22
Time Zone            : GMT +00:00
Daylight Saving Time : Disabled
Offset In Minutes    : 60
Repeating            : From : Apr 1st Sun 00:00
                    : To  : Oct last Sun 00:00
Annual              : From : 29 Apr 00:00
                    : To  : 12 Oct 00:00

DES-3528:5#
```

ARP AND GRATUITOUS 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 arpentry	<ipaddr> <macaddr>
config arpentry	<ipaddr> <macaddr>
delete arpentry	[<ipaddr> all]
show arpentry	{ipif <ipif_name 12> ipaddress <ipaddr> static}
config arp_aging time	[<sec 30-3932100> 0]
clear arptable	
config arp_spoofing_prevention	[add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> all] delete gateway_ip <ipaddr>]
show arp_spoofing_prevention	
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.

create arpentry

Purpose	Used to make a static entry into the ARP table.
Syntax	create arpentry <ipaddr> <macaddr>
Description	This command is used to enter an IP address and the corresponding MAC address into the Switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. <macaddr> – The MAC address corresponding to the IP address above.
Restrictions	Only Administrator and Operator-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-3528:5#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DES-3528:5#
```

config arpentry

Purpose	Used to configure a static entry in the ARP table.
Syntax	config arpentry <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.
Restrictions	Only Administrator and Operator-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-3528:5#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-3528:5#
```

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 <i>all</i> clears the Switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. <i>all</i> – Deletes all ARP entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

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

```
DES-3528:5#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-3528:5#
```

config arp_aging time

Purpose	Used to configure the age-out timer for ARP table entries on the Switch.
Syntax	config arp_aging time [<sec 30-3932100> 0]
Description	This command sets the maximum amount of time, in seconds, that an ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	<i>time</i> [<sec 30-3932100> 0]– The ARP age-out time, in seconds. The value may be set in the range of 0, or 30 to 3932100 seconds with a default setting of 1200 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```
DES-3528:5#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3528:5#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	show arpentry {ipif <ipif_name 12> ipaddress <ipaddr> static }
Description	This command is used to display the current contents of the Switch's ARP table.
Parameters	<i>ipif</i> <ipif_name 12> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. <i>ipaddress</i> <ipaddr> – The network address corresponding to the IP interface name above. <i>static</i> – Displays the static entries to the ARP table.
Restrictions	None.

Example Usage:

To display the ARP table:

```
DES-3528:5#show arpentry
Command: show arpentry

ARP Aging Time : 1200

Interface      IP Address      MAC Address      Type
-----
System         10.0.0.0        FF-FF-FF-FF-FF-FF Local/Broadcast
System         10.1.1.164      00-50-BA-70-E4-65 Dynamic
System         10.1.1.254      00-03-09-18-10-01 Dynamic
System         10.1.104.222    00-04-00-00-00-00 Dynamic
System         10.2.87.62      00-50-BA-66-77-56 Dynamic
System         10.5.2.5        00-E0-18-D4-63-1C Dynamic
System         10.6.51.98      00-1D-60-E7-B5-CD Dynamic
System         10.9.68.89      00-13-65-61-A0-00 Dynamic
System         10.10.2.190     00-0F-3D-84-A0-0C Dynamic
System         10.10.27.66     00-80-C8-58-72-1B Dynamic
System         10.10.73.21     00-1E-58-4F-FE-60 Local
System         10.16.88.75     00-1C-F0-79-CA-13 Dynamic
System         10.20.20.8      00-17-31-ED-E4-5D Dynamic
System         10.20.20.61     00-00-81-9A-F2-F4 Dynamic
System         10.38.65.65     00-50-BA-DA-01-58 Dynamic
System         10.41.44.251    08-00-28-32-00-AC Dynamic
System         10.43.47.55     00-07-E9-13-9B-DC Dynamic
```

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

clear arptable

Purpose	Used to remove all dynamic ARP table entries.
Syntax	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 and Operator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
DES-3528:5#clear arptable
Command: clear arptable

Success.

DES-3528:5#
```

config arp_spoofing_prevention

Purpose	Used to config to prevent ARP spoofing attack.
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 spoofing prevention entry so as to prevent the spoofing of protected gateway's MAC address. When an entry is created, if the sender IP of the ARP packet matches the gateway IP of the entry, but the sender MAC field and source MAC field do not match the gateway's MAC, then MAC of the entry will be dropped by the Switch.
Parameters	<p><i>add gateway_ip <ipaddr></i> – Specifies a gateway ip to be configured.</p> <p><i>add gateway_mac <macaddr></i> – Specifies a gateway mac to be configured.</p> <p><i>ports <portlist></i> - Specifies a port or range of ports to be configured.</p> <p><i>ports all</i> – Specifies all of ports to be configured.</p> <p><i>delete gateway_ip</i> – Specifies a gateway ip to be removed.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To add an entry for ARP spoofing prevention:

```
DES-3528:5# 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-3528:5#
```

show arp_spoofing_prevention

Purpose	Used to show the arp_spoofing_prevention entry.
Syntax	show arp_spoofing_prevention
Description	This command is used to display the current ARP spoofing prevention entry.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To add an entry for ARP spoofing prevention:

```
DES-3528:5# show arp_spoofing_prevention
Command: show arp_spoofing_prevention

ARP Spoofing Prevention Table
Gateway IP Address Gateway MAC Address   Ports
-----
10.254.254.251      00-00-00-11-11-11   1-2Total

Total Entries : 1

DES-3528:5#
```

config gratuitous_arp send ipif_status_up

Purpose	Used to enable/disable the sending of gratuitous ARP requests while the IP interface status comes up.
Syntax	config gratuitous_arp send ipif_status_up [enable disable]
Description	The command is used to enable/disable sending of gratuitous ARP request packets while the IPIF interface comes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is disabled.
Parameters	<i>enable</i> – Enable sending of gratuitous ARP when IPIF status comes up. <i>disable</i> – Disable sending of gratuitous ARP when IPIF status comes up.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable send gratuitous ARP request in a normal situation:

```
DES-3528:5#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DES-3528:5#
```

config gratuitous_arp send dup_ip_detected

Purpose	Used to enable/disable the sending of gratuitous ARP requests while a duplicate IP address is being detected.
Syntax	config gratuitous_arp send duplicate_ip_detected [enable disable]
Description	The command is used to enable/disable the sending of gratuitous ARP request packets when a duplicate IP has been detected. By default, the state is disabled. For this command, the duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address. In this case, the system knows that somebody is using an IP address that is in conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.
Parameters	<i>enable</i> – Enable sending of gratuitous ARP when a duplicate IP is detected. <i>disable</i> – Disable sending of gratuitous ARP when a duplicate IP is detected.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To enable send a gratuitous ARP request when a duplicate IP is detected:

```
DES-3528:5#config gratuitous_arp send duplicate_ip_detected enable
Command: config gratuitous_arp send duplicate_ip_detected enable

Success.

DES-3528:5#
```

config gratuitous_arp learning

Purpose	Used to enable/disable the learning of ARP entries in the ARP cache based on the received gratuitous ARP packets.
Syntax	config gratuitous_arp learning [enable disable]
Description	The command is used to enable/disable updating the ARP cache based on the received gratuitous ARP packets. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for. Note that, with the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet. By default, the state is disabled.
Parameters	<i>enable</i> – Enable learning of ARP entry based on the received gratuitous ARP packet. <i>disable</i> – Disable learning of ARP entry based on the received gratuitous ARP packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable learning of ARP entry based on the received gratuitous ARP packet:

```
DES-3528:5#config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DES-3528:5#
```

enable gratuitous_arp trap & log

Purpose	Used to enable gratuitous ARP trap and log state.
Syntax	enable gratuitous_arp {ipif <ipif_name 12>} {trap log }(1)
Description	The command is used to enable gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is disabled.
Parameters	<i>ipif <ipif_name 12></i> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. <i>{trap log}</i> – Select gratuitous ARP trap and/or log state.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable system interface's gratuitous ARP log and trap:

```
DES-3528:5#enable gratuitous_arp System trap log
Command: enable gratuitous_arp System trap log

Success.

DES-3528:5#
```


disable gratuitous_arp trap & log

Purpose	Used to disable gratuitous ARP trap and log state.
Syntax	disable gratuitous_arp {ipif <ipif_name 12>} {trap log }(1)
Description	This command is used to disable gratuitous ARP trap and log state. When the trap and log are disabled, the switch won't trap and log IP conflict events to inform the administrator.
Parameters	<i>ipif <ipif_name 12></i> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. <i>{trap log}</i> – Select gratuitous ARP trap and/or log state.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To disable the system interface's gratuitous ARP log and trap:

```
DES-3528:5#disable gratuitous_arp System trap log
Command: disable gratuitous_arp System trap log

Success.

DES-3528:5#
```

config gratuitous_arp send periodically

Purpose	Used to configure the interval for periodical sending of gratuitous ARP request packet.
Syntax	config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>
Description	The command is used to configure the interval for the periodic sending of gratuitous ARP request packets. By default, the interval is 0.
Parameters	<ipif_name 12> – The name of the Layer 3 interface. <value 0-65535> – Periodically send gratuitous ARP interval time in seconds. 0 – means not to send gratuitous ARP periodically.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure gratuitous ARP interval to 5 for IPIF System:

```
DES-3528:5#config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DES-3528:5#
```

show gratuitous arp

Purpose	Used to display gratuitous ARP configuration.
Syntax	show gratuitous_arp {ipif <ipif_name>}
Description	This command is used to display gratuitous ARP configuration.
Parameters	<ipif_name 12> – The interface name of the Layer 3 device.
Restrictions	None.

Example usage:

To display gratuitous ARP log and trap state:

```
DES-3528:5#show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF Status Up      : Disabled
Send on Duplicate_IP_Detected : Disabled
Gratuitous ARP Learning     : Disabled

IP Interface Name : System
  Gratuitous ARP Trap      : Disabled
  Gratuitous ARP Log       : Disabled
  Gratuitous ARP Periodical Send Interval : 0

Total Entries: 1

DES-3528:5#
```

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	

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	<p><i>default</i> – Specifies to create an IP route entry.</p> <p><i><ipaddr></i> – The gateway IP address for the next hop router.</p> <p><i><metric 1-65535></i> – 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.</p>
Restrictions	Only Administrator and Operator-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-3528:5#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DES-3528:5#
```

delete iproute

Purpose	Used to delete a default IP route entry from the Switch's IP routing table.
Syntax	delete iproute [default]
Description	This command will delete an existing default entry from the Switch's IP routing table.
Parameters	<i>default</i> – Specifies to delete a default IP route entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the default Gateway from the routing table:

```
DES-3528:5# delete iproute default
Command: delete iproute default

Success.

DES-3528:5#
```

show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	show iproute
Description	This command will display the Switch's current IP routing table.
Parameters	None.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DES-3528:5#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface        Cost    Protocol
-----
10.0.0.0/8          0.0.0.0          System           1       Local

Total Entries : 1

DES-3528:5#
```

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 and Operator-level users can issue this command.

Example usage:

To enable MAC notification without changing basic configuration:

```
DES-3528:5#enable mac_notification
Command: enable mac_notification

Success.

DES-3528:5#
```

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 and Operator-level users can issue this command.

Example usage:

To disable MAC notification without changing basic configuration:

```
DES-3528:5#disable mac_notification
Command: disable mac_notification

Success.

DES-3528:5#
```

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	<i>interval <sec 1-2147483647></i> – The time in seconds between notifications. The user may choose an interval between 1 and 2,147,483,647 seconds. <i>historysize <1-500></i> – The maximum number of entries listed in the history log used for notification.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DES-3528:5#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DES-3528:5#
```

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	<i><portlist></i> – Specify a port or range of ports to be configured. <i>all</i> – Entering this command will set all ports on the system. <i>[enable disable]</i> – These commands will enable or disable MAC address table notification on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DES-3528:5#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-3528:5#
```

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-3528:5#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State           : Enabled
Interval        : 1
History Size    : 1

DES-3528:5#
```

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 the MAC address table notification status settings for ports 1-7:

```
DES-3528:5#show mac_notification ports 1-7
Command: show mac_notification ports 1-7

Port #  MAC Address Table Notification State
-----  -----
1                Disabled
2                Disabled
3                Disabled
4                Disabled
5                Disabled
6                Disabled
7                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:

- A) The server verifies the username and password, and the user is granted normal user privileges on the Switch.
- B) The server will not accept the username and password and the user is denied access to the Switch.
- C) 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, which is only available for logging in the Switch from the three versions of the TACACS server, 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 will 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-3528:5#enable authen_policy
Command: enable authen_policy

Success.

DES-3528:5#
```

disable authen_policy

Purpose	Used to disable system access authentication policy.
Syntax	disable authen_policy
Description	This command will 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-3528:5#disable authen_policy
Command: disable authen_policy

Success.

DES-3528:5#
```

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-3528:5#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DES-3528:5#
```

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	<i><string 15></i> – Enter an alphanumeric string of up to 15 characters to define the given <i>method list</i> .
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the method list “Trinity.”:

```
DES-3528:5#create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity

Success.

DES-3528:5#
```

config authen_login

Purpose	Used to configure a user-defined or default method list of authentication 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	<p>This command will 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 <i>tacacs – xtacacs – local</i>, the Switch will send an authentication request to the first <i>tacacs</i> host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second <i>tacacs</i> 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, <i>xtacacs</i>. If no authentication takes place using the <i>xtacacs</i> list, the <i>local</i> 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.</p> <p>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.)</p>
Parameters	<p><i>default</i> – The default method list for access authentication, as defined by the user. The user may choose one or a combination of up to four of the following authentication methods:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Adding this parameter will require the user to be authenticated using the

config authen_login

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.
- *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 “Trinity” with authentication methods TACACS, XTACACS and local.

```
DES-3528:5#config authen_login method_list_name Trinity method tacacs xtacacs local
Command: config authen_login method_list_name Trinity method tacacs xtacacs local
```

Success.

```
DES-3528:5#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DES-3528:5#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

DES-3528:5#
```

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	<i><string 15></i> – Enter an alphanumeric string of up to 15 characters to define the given <i>method list</i> the user wishes to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the method list name “Trinity”:

```
DES-3528:5#delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DES-3528:5#
```

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><i>default</i> – Entering this parameter will display the default method list for users logging on to the Switch.</p> <p><i>method_list_name <string 15></i> – Enter an alphanumeric string of up to 15 characters to define the given method list to view.</p> <p><i>all</i> – 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> <ul style="list-style-type: none"> ▪ <i>Method List Name</i> – The name of a previously configured method list name. ▪ <i>Priority</i> – 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). ▪ <i>Method Name</i> – Defines which security protocols are implemented, per method list name. ▪ <i>Comment</i> – Defines the type of Method. <i>User-defined Group</i> refers to server group defined by the user. <i>Built-in Group</i> refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. <i>Keyword</i> 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).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the authentication login method list named Trinity:

```
DES-3528:5#show authen_login method_list_name Trinity
Command: show authen_login method_list_name Trinity

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

DES-3528:5#
```

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 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	<i><string 15></i> – Enter an alphanumeric string of up to 15 characters to define the given <i>enable method list</i> 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-3528:5#create authen_enable method_list_name Permit
Command: create authen_enable method_list_name Permit

Success.

DES-3528:5#
```

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 <i>tacacs – xtacacs – local_enable</i>, 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, <i>xtacacs</i>. If no authentication takes place using the <i>xtacacs</i> list, the <i>local_enable</i> 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><i>default</i> – 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 (4) of the following authentication methods:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from the remote TACACS <i>server hosts</i> of the TACACS <i>server group</i> list. ▪ <i>xtacacs</i> – Adding this parameter will require the user to be authenticated using the XTACACS protocol from the remote XTACACS <i>server hosts</i> of the XTACACS <i>server group</i> list. ▪ <i>tacacs+</i> – Adding this parameter will require the user to be authenticated using the

config authen_enable

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_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 (4) 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.

```
DES-3528:5#config authen_enable method_list_name Trinity method tacacs xtacacs local
Command: config authen_enable method_list_name Trinity method tacacs xtacacs local
Success.
```

```
DES-3528:5#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DES-3528:5#config authen_enable default method xtacacs tacacs+ local
Command: config authen_enable default method xtacacs tacacs+ local
```

```
Success.
```

```
DES-3528:5#
```


delete authen_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 authen_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	<i><string 15></i> – Enter an alphanumeric string of up to 15 characters to define the given <i>enable method list</i> to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user-defined method list “Permit”

```
DES-3528:5#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DES-3528:5#
```

show authen_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 authen_enable [default method_list_name <string 15> all]
Description	This command is used to display a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	<p><i>default</i> – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the Switch.</p> <p><i>method_list_name <string 15></i> – Enter an alphanumeric string of up to 15 characters to define the given <i>method list</i> the user wishes to view.</p> <p><i>all</i> – 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> <ul style="list-style-type: none"> ▪ <i>Method List Name</i> – The name of a previously configured method list name. ▪ <i>Priority</i> – 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). ▪ <i>Method Name</i> – Defines which security protocols are implemented, per method list name. ▪ <i>Comment</i> – Defines the type of Method. <i>User-defined Group</i> refers to <i>server groups</i> defined by the user. <i>Built-in Group</i> refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. <i>Keyword</i> refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the <i>local_enable</i> 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-3528:5#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	Darren	User-defined Group
	4	local	Keyword
default	1	tacacs+	Built-in Group
	2	local	Keyword

```
Total Entries : 2
```

```
DES-3528:5#
```

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 (<i>authen_enable</i>) utilizing a previously configured method list.
Parameters	<p><i>application</i> – Choose the application to configure. The user may choose one of the following five options to configure.</p> <ul style="list-style-type: none"> ▪ <i>console</i> – Choose this parameter to configure the command line interface login method. ▪ <i>telnet</i> – Choose this parameter to configure the telnet login method. ▪ <i>ssh</i> – Choose this parameter to configure the Secure Shell login method. ▪ <i>http</i> – Choose this parameter to configure the web interface login method. ▪ <i>all</i> – Choose this parameter to configure all applications (console, telnet, ssh, web) login method. <p><i>login</i> – Use this parameter to configure an application for normal login on the user level, using a previously configured method list.</p> <p><i>enable</i> – Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list.</p> <p><i>default</i> – Use this parameter to configure an application for user authentication using the default method list.</p> <p><i>method_list_name <string 15></i> – Use this parameter to configure an application for user authentication using a previously configured method list. Enter a alphanumeric string of up to 15 characters to define a previously configured method list.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the web interface:

```
DES-3528:5#config authen application http login default
```

```
Command: config authen application http login default
```

```
Success.
```

```
DES-3528:5#
```

show authen application

Purpose	Used to display authentication methods for the various applications on the Switch.
Syntax	show authen application
Description	This command will 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-3528:5#show authen application
Command: show authen application

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

DES-3528:5#
```

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 1-255> retransmit < 1-255>}
Description	This command will 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><i>server_host</i> <ipaddr> – The IP address of the remote server host to add.</p> <p><i>protocol</i> – The protocol used by the server host. The user may choose one of the following:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Enter this parameter if the server host utilizes the TACACS protocol. ▪ <i>xtacacs</i> – Enter this parameter if the server host utilizes the XTACACS protocol. ▪ <i>tacacs+</i> – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ <i>radius</i> – Enter this parameter if the server host utilizes the RADIUS protocol. <p><i>port</i> <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><i>key</i> <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><i>timeout</i> <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><i>retransmit</i> <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-3528:5#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-3528:5#
```

config authen server_host

Purpose	Used to configure a user-defined authentication 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 will 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><i>server_host</i> <ipaddr> – The IP address of the remote server host the user wishes to alter.</p> <p><i>protocol</i> – The protocol used by the server host. The user may choose one of the following:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Enter this parameter if the server host utilizes the TACACS protocol. ▪ <i>xtacacs</i> – Enter this parameter if the server host utilizes the XTACACS protocol. ▪ <i>tacacs+</i> – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ <i>radius</i> – Enter this parameter if the server host utilizes the RADIUS protocol. <p><i>port</i> <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><i>key</i> <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><i>timeout</i> <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><i>retransmit</i> <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-3528:5#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-3528:5#
```

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><i>server_host</i> <ipaddr> – The IP address of the remote server host to be deleted.</p> <p><i>protocol</i> – The protocol used by the server host the user wishes to delete. The user may choose one of the following:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Enter this parameter if the server host utilizes the TACACS protocol. ▪ <i>xtacacs</i> – Enter this parameter if the server host utilizes the XTACACS protocol. ▪ <i>tacacs+</i> – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ <i>radius</i> – Enter this parameter if the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a user-defined TACACS+ authentication server host:

```
DES-3528:5#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DES-3528:5#
```

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><i>IP Address</i> – The IP address of the authentication server host.</p> <p><i>Protocol</i> – The protocol used by the server host. Possible results will include TACACS, XTACACS, TACACS+ or RADIUS.</p> <p><i>Port</i> – The virtual port number on the server host. The default value is 49.</p> <p><i>Timeout</i> – The time in seconds the Switch will wait for the server host to reply to an authentication request.</p> <p><i>Retransmit</i> – 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.</p> <p><i>Key</i> – Authentication key to be shared with a configured TACACS+ server only.</p>
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DES-3528:5#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-3528:5#
```

create authen server_group

Purpose	Used to create a user-defined authentication server group.
Syntax	create authen server_group <string 15>
Description	This command will 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	<i><string 15></i> – 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-3528:5#create authen server_group group_1
Command: create authen server_group group_1

Success.

DES-3528:5#
```

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 will 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><i>server_group</i> – 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> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – 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. ▪ <i>xtacacs</i> – 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. ▪ <i>tacacs+</i> – 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. ▪ <i>radius</i> – 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. ▪ <i><string 15></i> – 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><i>add/delete</i> – Enter the correct parameter to add or delete a server host from a server group.</p> <p><i>server_host <ipaddr></i> – Enter the IP address of the previously configured server host to add or delete.</p> <p><i>protocol</i> – Enter the protocol utilized by the server host. There are three options:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Use this parameter to define the protocol if the server host is using the TACACS authentication protocol. ▪ <i>xtacacs</i> – Use this parameter to define the protocol if the server host is using the XTACACS authentication protocol. ▪ <i>tacacs+</i> – Use this parameter to define the protocol if the server host is using the TACACS+ authentication protocol. ▪ <i>radius</i> – Use this parameter to define the protocol if the server host is using the RADIUS authentication protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add an authentication host to server group “group_1”:

```
DES-3528:5# config authen server_group group_1 add server_host 10.1.1.121 protocol
tacacs+
Command: config authen server_group group_1 add server_host 10.1.1.121 protocol
tacacs+

Success.

DES-3528:5#
```


delete authen server_group

Purpose	Used to delete a user-defined authentication server group.
Syntax	delete authen server_group <string 15>
Description	This command will 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-3528:5#delete server_group group_1
Command: delete server_group group_1

Success.

DES-3528:5#
```

show authen server_group

Purpose	Used to view authentication server groups on the Switch.
Syntax	show authen server_group <string 15>
Description	This command will 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	Only Administrator-level users can issue this command.

Example usage:

To view authentication server groups currently set on the Switch.

```
DES-3528:5#show authen server_group
```

```
Command: show authen server_group
```

```
Server Group : mix_1
```

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

```
Total Entries : 5
```

```
DES-3528:5#
```

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 will set the time the Switch will wait for a response of authentication from the user.
Parameters	<i>response_timeout <int 0-255></i> – 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. Zero means there won't be a time-out. The default value is 0 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the response timeout for 60 seconds:

```
DES-3528:5#config authen parameter response_timeout 60
```

```
Command: config authen parameter response_timeout 60
```

```
Success.
```

```
DES-3528:5#
```

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 will 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	<i>parameter attempt <int 1-255></i> – Set the maximum number of attempts the user may try to become authenticated by the Switch, before being locked out. The default setting is 3.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the maximum number of authentication attempts at 5:

```
DES-3528:5#config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DES-3528:5#
```

show authen parameter

Purpose	Used to display the authentication parameters currently configured on the Switch.
Syntax	show authen parameter
Description	This command will display the authentication parameters currently configured on the Switch, including the response timeout and user authentication attempts. This command will display the following fields: 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. User attempts: The maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.
Parameters	None.
Restrictions	None.

Example usage:

To view the authentication parameters currently set on the Switch:

```
DES-3528:5#show authen parameter
Command: show authen parameter

Response Timeout : 30 seconds
User Attempts    : 3

DES-3528:5#
```

enable admin

Purpose	Used to promote user level privileges to administrator level privileges.
Syntax	enable admin
Description	This command is for users who have logged on to the Switch with the normal user privilege and can be switched to the admin privilege. 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 (<i>none</i>). 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.
Parameters	None.
Restrictions	None.

Example usage:

To enable administrator privileges on the Switch:

```
DES-3528:5#enable admin
Password: *****

DES-3528:5#
```

config admin local_enable

Purpose	Used to configure the local enable password for administrator level privileges.
Syntax	config admin local_enable
Description	This command will 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	<i><password 15></i> – 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-3528:5#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-3528:5#
```

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
enable ssh	
disable ssh	
config ssh authmode	[password publickey hostbased] [enable disable]
show ssh authmode	
config ssh server	{maxsession <int 1-8> contimeout <sec 120-600> authfail<int 2-20> rekey [10min 30min 60min never] port <tcp_port_number 1-65535>}(1)
show ssh server	
config ssh user	<username> authmode [hostbased [hostname <domain_name> hostname_IP <domain_name> <ipaddr>] password publickey]
show ssh user authmode	
config ssh algorithm	[3DES AES128 AES192 AES256 arcfour blowfish cast128 twofish128 twofish192 twofish256 MD5 SHA1 RSA DSA] [enable disable]
show ssh algorithm	

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

enable ssh

Purpose	Used to enable SSH.
Syntax	enable ssh
Description	This command allows users to enable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To enable SSH:

```
enable ssh
```

```
Command: enable ssh
```

```
TELNET will be disabled when enable SSH.
```

```
Success.
```

```
DES-3528:5#
```

disable ssh

Purpose	Used to disable SSH.
Syntax	disable ssh
Description	This command allows users to disable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To disable SSH:

```
DES-3528:5#disable ssh
```

```
Command: disable ssh
```

```
Success.
```

```
DES-3528:5#
```

config ssh authmode

Purpose	Used to configure the SSH authentication mode setting.
Syntax	config ssh authmode [password publickey hostbased] [enable disable]
Description	This command will allow users to configure the SSH authentication mode for users attempting to access the Switch.
Parameters	<p><i>password</i> – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the Switch.</p> <p><i>publickey</i> – This parameter may be chosen if the administrator wishes to use a publickey configuration set on a SSH server, for authentication.</p> <p><i>hostbased</i> – 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><i>[enable disable]</i> – This allows users to enable or disable SSH authentication on the Switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DES-3528:5#config ssh authmode password enable
```

```
Command: config ssh authmode password enable
```

```
Success.
```

```
DES-3528:5#
```

show ssh authmode

Purpose	Used to display the SSH authentication mode setting.
Syntax	show ssh authmode
Description	This command will allow users 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-3528:5#show ssh authmode
```

```
Command: show ssh authmode
```

```
The SSH Authmode:
```

```
-----
Password      : Enabled
Publickey     : Enabled
Hostbased     : Enabled
```

```
DES-3528:5#
```

config ssh server

Purpose	Used to configure the SSH server.
Syntax	config ssh server {maxsession <int 1-8> contimeout <sec 120-600> authfail<int 2-20> rekey [10min 30min 60min never] port <tcp_port_number 1-65535>}(1)
Description	This command allows users to configure the SSH server.
Parameters	<p><i>maxsession <int 1-8></i> – Allows the user to set the number of users that may simultaneously access the Switch. The default setting is 8.</p> <p><i>contimeout <sec 120-600></i> – 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><i>authfail <int 2-20></i> – 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><i>rekey [10min 30min 60min never]</i> – Sets the time period that the Switch will change the security shell encryptions.</p> <p><i>tcp_port_number 1-65535</i> – Specifies the TCP port used to communicate between SSH client and server. The default value is 22.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To configure the SSH server:

```
DES-3528:5#config ssh server maxsession 2 contimeout 300 authfail 2
```

```
Command: config ssh server maxsession 2 contimeout 300 authfail 2
```

```
Success.
```

```
DES-3528:5#
```

show ssh server

Purpose	Used to display the SSH server setting.
Syntax	show ssh server
Description	This command allows users to display the current SSH server setting.
Parameters	None.
Restrictions	None.

Usage example:

To display the SSH server:

```
DES-3528:5#show ssh server
Command: show ssh server

The SSH Server Configuration
Max Session           : 8
Connection Timeout   : 120
Authfail Attempts    : 2
Tcp Port Number      : 22
Rekey Timeout        : Never

DES-3528:5#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	config ssh user <username 15> authmode [hostbased [hostname <domain_name> hostname_IP <domain_name> <ipaddr >] password publickey]
Description	This command allows users to configure the SSH user authentication method.
Parameters	<p><i><username 15></i> – Enter a username of no more than 15 characters to identify the SSH user.</p> <p><i>authmode</i> – 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"> <i>hostbased</i> – 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. <ul style="list-style-type: none"> • <i>hostname <domain_name></i> – Enter an alphanumeric string of up to 32 characters identifying the remote SSH user. • <i>hostname_IP <domain_name> <ipaddr></i> – Enter the hostname and the corresponding IP address of the SSH user. <i>password</i> – This parameter should be chosen to use an administrator defined password for authentication. <i>publickey</i> – 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-3528:5#config ssh user Trinity authmode password
Command: config ssh user Trinity authmode password

Success.

DES-3528:5#
```

show ssh user authmode

Purpose	Used to display the SSH user setting.
Syntax	show ssh user authmode
Description	This command allows users 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-3528:5#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
Username      AuthMode      HostName      HostIP
-----      -
123           Password

Total Entries : 1

DES-3528:5#
```



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 allows users to configure the desired type of SSH algorithm used for authentication encryption.
Parameters	<p><i>3DES</i> – This parameter will enable or disable the Triple_Data Encryption Standard encryption algorithm.</p> <p><i>AES128</i> – This parameter will enable or disable the Advanced Encryption Standard AES128 encryption algorithm.</p> <p><i>AES192</i> – This parameter will enable or disable the Advanced Encryption Standard AES192 encryption algorithm.</p> <p><i>AES256</i> – This parameter will enable or disable the Advanced Encryption Standard AES256 encryption algorithm.</p> <p><i>arcfour</i> – This parameter will enable or disable the Arcfour encryption algorithm.</p> <p><i>blowfish</i> – This parameter will enable or disable the Blowfish encryption algorithm.</p> <p><i>cast128</i> – This parameter will enable or disable the Cast128 encryption algorithm.</p> <p><i>twofish128</i> – This parameter will enable or disable the twofish128 encryption algorithm.</p> <p><i>twofish192</i> – This parameter will enable or disable the twofish192 encryption algorithm.</p> <p><i>MD5</i> – This parameter will enable or disable the MD5 Message Digest encryption algorithm.</p> <p><i>SHA1</i> – This parameter will enable or disable the Secure Hash Algorithm encryption.</p> <p><i>RSA</i> – This parameter will enable or disable the RSA encryption algorithm.</p> <p><i>DSA</i> – This parameter will enable or disable the Digital Signature Algorithm encryption.</p> <p><i>[enable disable]</i> – This allows the user to enable or disable algorithms entered in this command, on the Switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To configure SSH algorithm:

```
DES-3528:5#config ssh algorithm blowfish enable
Command: config ssh algorithm blowfish enable

Success.

DES-3528:5#
```

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.
Parameters	None.
Restrictions	None.

Usage Example:

To display SSH algorithms currently set on the Switch:

```
DES-3528:5#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
```

```
DES-3528:5#
```

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:

1. **Key Exchange:** The first part of the cyphersuite 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.
2. **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.
3. **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.

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}}
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}}
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	Used 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}}
Description	This command will 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><i>ciphersuite</i> – 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><i>RSA_with_RC4_128_MD5</i> – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm.</p> <p><i>RSA_with_3DES_EDE_CBC_SHA</i> – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm.</p> <p><i>DHE_DSS_with_3DES_EDE_CBC_SHA</i> – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm.</p> <p><i>RSA_EXPORT_with_RC4_40_MD5</i> – 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-3528:5#enable ssl
```

```
Command: enable ssl
```

```
Note: Web will be disabled if SSL is enabled.
```

```
Success.
```

```
DES-3528:5#
```



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	Used 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}}
Description	This command will disable SSL on the Switch and can be used to disable any one or combination of listed ciphersuites on the Switch.
Parameters	<p><i>ciphersuite</i>– 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><i>RSA_with_RC4_128_MD5</i> – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm.</p> <p><i>RSA_with_3DES_EDE_CBC_SHA</i> – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm.</p> <p><i>DHE_DSS_with_3DES_EDE_CBC_SHA</i> – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm.</p> <p><i>RSA_EXPORT_with_RC4_40_MD5</i> – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DES-3528:5#disable ssl
```

```
Command: disable ssl
```

```
Success.
```

```
DES-3528:5#
```

To disable ciphersuite RSA_EXPORT_with_RC4_40_MD5 only:

```
DES-3528:5#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
```

```
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
```

```
Success.
```

```
DES-3528:5#
```

config ssl cachetimeout

Purpose	Used to configure the SSL cache timeout.
Syntax	config ssl cachetimeout timeout <value 60-86400>
Description	This command will 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	<i>timeout <value 60-86400></i> – 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-3528:5#config ssl cachetimeout 7200
Command: config ssl cachetimeout 7200

Success.

DES-3528:5#
```

show ssl cachetimeout

Purpose	Used to show the SSL cache timeout.
Syntax	show ssl cachetimeout
Description	This command allows the user 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-3528:5#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DES-3528:5#
```

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-3528:5#show ssl
Command: show ssl

SSL status           Enabled
RSA_WITH_RC4_128_MD5 Enabled
RSA_WITH_3DES_EDE_CBC_SHA Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA Enabled
RSA_EXPORT_WITH_RC4_40_MD5 Enabled

DES-3528:5#
```

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-3528:5#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DES-3528:5#
```

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 about 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	<p><i><ipaddr></i> – Enter the IP address of the TFTP server.</p> <p><i>certfilename <path_filename 64></i> – Enter the path and the filename of the certificate file users wish to download.</p> <p><i>keyfilename <path_filename 64></i> – Enter the path and the filename of the key exchange file users wish to download.</p> <p><i>path_filename</i> – Private key file path respect to tftp server root path, and input characters max to 64 octets.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download a certificate file and key file to the Switch:

```
DES-3528:5#DES-3528:5# download ssl certificate 10.55.47.1 certfilename cert.der
keyfilename pkey.der
Command: download ssl certificate 10.55.47.1 certfilename cert.der keyfilename
pkey.der

Success.

DES-3528:5#
```


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 are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DES-3528 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 DES-3528, 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:

1. Each device begins in the Commander state.
2. 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.
3. The user can manually configure a CS to become a CaS.
4. A MS can become a CaS by:
 - a. Being configured as a CaS through the CS.
 - b. If report packets from the CS to the MS time out.
5. The user can manually configure a CaS to become a CS
6. 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 DES-3528 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, 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 (include read/write and read only) to which the CS belongs. However if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

The Upgrade to v1.6

To better improve SIM management, the xStack DES-3528 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 SIM 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 will 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-3528:5#enable sim
Command: enable sim

Success.

DES-3528:5#
```

disable sim

Purpose	Used to disable Single IP Management (SIM) on the Switch
Syntax	disable sim
Description	This command will 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-3528:5#disable sim
Command: disable sim

Success.

DES-3528:5#
```

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 will display the current information regarding the SIM group on the Switch, including the following:</p> <p><i>SIM Version</i> – Displays the current Single IP Management version on the Switch.</p> <p><i>Firmware Version</i> – Displays the current Firmware version on the Switch.</p> <p><i>Device Name</i> – Displays the user-defined device name on the Switch.</p> <p><i>MAC Address</i> – Displays the MAC Address of the Switch.</p> <p><i>Capabilities</i> – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3).</p> <p><i>Platform</i> – Switch Description including name and model number.</p> <p><i>SIM State</i> – Displays the current Single IP Management State of the Switch, whether it be enabled or disabled.</p> <p><i>Role State</i> – 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><i>Discovery Interval</i> – Time in seconds the Switch will send discovery packets out over the network.</p> <p><i>Hold time</i> – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.</p>
Parameters	<p><i>candidates</i> <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><i>members</i> <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><i>group</i> {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><i>neighbor</i> – 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> <ul style="list-style-type: none"> Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located. MAC Address – Displays the MAC Address of the neighbor switch. Role – Displays the role(CS, CaS, MS) of the neighbor switch.
Restrictions	None.

Example usage:

To show the SIM information in detail:

```
DES-3528:5#show sim
Command: show sim

SIM Version       : VER-1.61
Firmware Version  : 1.03.B008
Device Name       :
MAC Address       : 00-21-91-AF-EA-00
Capabilities      : L2
Platform          : DES-3528 L2 Switch
SIM State         : Disabled
Role State        : Candidate
Discovery Interval : 30 sec
Hold Time         : 100 sec

DES-3528:5#
```

To show the candidate information in summary, if the candidate ID is specified:

```
DES-3528:5#show sim candidates
Command: show sim candidates

ID  MAC Address           Platform /           Hold   Firmware   Device Name
---  -
1   00-01-02-03-04-00    DES-3526 L2 Switch  40     1.03.B008  The Man
2   00-55-55-00-55-00    DES-3526 L2 Switch  140    1.03.B008  default

Total Entries: 2

DES-3528:5#
```

To show the member information in summary:

```
DES-3528:5#show sim members
Command: show sim members

ID  MAC Address           Platform /           Hold   Firmware   Device Name
---  -
1   00-01-02-03-04-00    DES-3528 L2 Switch  40     1.00.B008  The Man
2   00-55-55-00-55-00    DES-3528 L2 Switch  140    1.00.B008  default master

Total Entries: 2

DES-3528:5#
```

To show other groups information in summary, if group is specified:

```
DES-3528:5#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address          Platform /
   -----          -----
*1  00-01-02-03-04-00    DES-3528 L2 Switch    40    1.00.B008    Trinity
 2  00-55-55-00-55-00    DES-3528 L2 Switch    140   1.00.B008    default master

SIM Group Name : SIM2

ID  MAC Address          Platform /
   -----          -----
*1  00-01-02-03-04-00    DES-3528 L2 Switch    40    1.00.B008    Neo
 2  00-55-55-00-55-00    DES-3528 L2 Switch    140   1.00.B008    default master

DES-3528:5#
```

Example usage:

To view SIM neighbors:

```
DES-3528:5#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-3528:5#
```

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.
Parameters	<i>member_id</i> <value 1-32> – Select the ID number of the member switch to configure. <i>exit</i> – This command is used to exit from managing the member switch and will return to managing the commander switch.
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-3528:5#reconfig member_id 2
Command: reconfig member_id 2

DES-3528:5#
Login:
```

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><i>add <candidate_id> <password></i> – 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><i>delete <member_id 1-32></i> – 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-3528:5#config sim_group add 2
Command: config sim_group add 2

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

Success.

DES-3528:5#
```

To delete a member:

```
DES-3528:5#config sim delete 1
Command: config sim delete 1

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

DES-3528:5#
```

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 <30-90> hold_time <sec 100-255>]]
Description	This command is used to configure parameters of switches of the SIM.
Parameters	<p><i>commander</i> – Use this parameter to configure the commander switch (CS) for the following parameters:</p> <ul style="list-style-type: none"> ▪ <i>group_name</i> <groupname 64> – Used to update the name of the group. Enter an alphanumeric string of up to 64 characters to rename the SIM group. ▪ <i>dp_interval</i> <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 <i>dp_interval</i> from 30 to 90 seconds. ▪ <i>hold time</i> <sec 100-300> – Using this parameter, the user may set the time, in seconds, the CS will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 300 seconds. <p><i>candidate</i> – Used to change the role of a CS (commander) to a CaS (candidate).</p> <ul style="list-style-type: none"> ▪ <i>dp_interval</i> <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 <i>dp_interval</i> from 30 to 90 seconds. ▪ <i>hold time</i> <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-3528:5#config sim commander dp_interval 30
Command: config sim commander dp_interval 30

Success.

DES-3528:5#
```

To change the hold time of the discovery protocol:

```
DES-3528:5#config sim commander hold_time 120
Command: config sim commander hold_time 120

Success.

DES-3528:5#
```

To transfer the CS (commander) to be a CaS (candidate):

```
DES-3528:5#config sim candidate
Command: config sim candidate

Success.

DES-3528:5#
```


To transfer the Switch to be a CS:

```
DES-3528:5#config sim commander
Command: config sim commander

Success.

DES-3528:5#
```

To update the name of a group:

```
DES-3528:5#config sim commander group_name Trinity
Command: config sim commander group_name Trinity

Success.

DES-3528:5#
```

download sim_ms

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 will download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	<p><i>firmware_from_tftp</i> – Specify this parameter to download firmware to members of a SIM group.</p> <p><i>configuration_from_tftp</i> – Specify this parameter to download a switch configuration to members of a SIM group.</p> <p><i><ipaddr></i> – Enter the IP address of the TFTP server.</p> <p><i><path_filename></i> – Enter the path and the filename of the firmware or switch on the TFTP server.</p> <p><i>members</i> – 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> <ul style="list-style-type: none"> ▪ <i><mslist></i> – Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration. ▪ <i>all</i> – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download firmware:

```
DES-3528:5#download sim_ms firmware_from_tftp 10.53.13.94 c:/des3526.had members all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/des3526.had members all

This device is updating firmware. Please wait...

Download Status :
```

ID	MAC Address	Result
1	00-01-02-03-04-00	Success
2	00-07-06-05-04-03	Success
3	00-07-06-05-04-03	Success

```
DES-3528:5#
```

To download configuration files:

```
DES-3528:5#download sim_ms configuration_from_tftp 10.53.13.94 c:/des3528.txt
members all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/des3528.txt members all

This device is updating configuration. Please wait...

Download Status :
```

ID	MAC Address	Result
1	00-01-02-03-04-00	Success
2	00-07-06-05-04-03	Success
3	00-07-06-05-04-03	Success

```
DES-3528:5#
```

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 <mclist> all]}
Description	This command will upload a configuration file to a TFTP server from a specified member of a SIM group.
Parameters	<p><i>configuration_from_tftp</i> – Specify this parameter to upload a switch configuration to members of a SIM group.</p> <p><i>log_to_tftp</i> – Specify this parameter to upload a switch log to a member of the SIM group.</p> <p><i><ipaddr></i> – Enter the IP address of the TFTP server to which to upload a configuration file.</p> <p><i><path_filename></i> – Enter a user-defined path and file name on the TFTP server so as to upload configuration files.</p> <p><i>members</i> – Enter this parameter to specify the members to which the user prefers to upload the switch configuration or log files. The user may specify a member or members by adding one of the following:</p> <ul style="list-style-type: none"> ▪ <i><mclist></i> – Enter a value, or values to specify which members of the SIM group will upload the switch configuration or log. <p><i>all</i> – Add this parameter to specify all members of the SIM group will upload the switch configuration or log.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DES-3528:5#upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt
members 1
Command: upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt members
1

Success.

DES-3528:5#
```

JWAC COMMANDS

The Japanese Web-based Access Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable jwac	
disable jwac	
enable jwac redirect	
disable jwac redirect	
enable jwac forcible_logout	
disable jwac forcible_logout	
enable jwac udp_filtering	
disable jwac udp_filtering	
enable jwac quarantine_server_monitor	
disable jwac quarantine_server_monitor	
config jwac quarantine_server_error_timeout	<sec 5-300>
config jwac redirect	{destination [quarantine_server jwac_login_page] delay_time <sec 0 - 10>}(1)
config jwac virtual_ip	<ipaddr>
config jwac quarantine_server_url	<string 128>
config jwac clear_quarantine_server_url	
config jwac update_server	[add delete] ipaddress <network_address>
config jwac switch_http_port	< tcp_port_number 1-65535> {[http https]}
config jwac ports	[<portlist> all] {state [enable disable] max_authenticating_host <value 0 - 50> aging_time [infinite <min 1 - 1440>] idle_time [infinite <min 1 - 1440>] block_time [<sec 0 - 300>] auth_mode [host_based port_based] }(1)
config jwac radius_protocol	[local pap chap ms_chap ms_chapv2 eap_md5]
create jwac user	<username 15> {vlan <vlanid 1 - 4094>}
config jwac user	<username 15> {vlan <vlanid 1 - 4094>}
delete jwac	[user <username 15> all_users]
show jwac user	
clear jwac auth_state	[ports [all <portlist>] {authenticated authenticating blocked} mac_addr <macaddr>]
show jwac	
show jwac auth_state ports	<portlist>

Command	Parameters
show jwac ports	<portlist>
config jwac auth_failover	[enable disable]
config jwac authorization network	{radius [enable disable] local [enable disable]}(1)
config jwac authenticate_page	< Japanese english >
show jwac authenticate_page element	
config jwac authentication_page element	[japanese english] [default page_title <desc 128> login_window_title <desc 32> user_name_title <desc 16> password_title <desc 16> logout_window_title <desc 32>]

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

enable jwac	
Purpose	Used to enable JWAC function.
Syntax	enable jwac
Description	This command is used to enable JWAC function. JWAC and WAC are mutual exclusive functions. They cannot be enabled at the same time. Using the JWAC function, PC users need to pass two stages of authentication. The first stage is to do the authentication with the Quarantine Server and the second stage is the authentication with the switch. For the second stage, the authentication is similar to WAC, except that there is no port VLAN membership change by JWAC after a host passes authentication. The RADIUS server will share the server configuration defined by the 802.1X command set.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC:

DES-3528:5#enable jwac
Command: enable jwac
Success.
DES-3528:5#

disable jwac	
Purpose	Used to disable JWAC function.
Syntax	disable jwac
Description	This command is used to diable JWAC function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC:

```
DES-3528:5#disable jwac
Command: disable jwac

Success.

DES-3528:5#
```

enable jwac redirect

Purpose	Used to enable JWAC redirect function.
Syntax	enable jwac redirect
Description	This command is for the unauthenticated host to be redirected to the Quarantine Server when it tries to access a random URL, or JWAC login page in the Switch.
Parameters	None.
Restrictions	When enabling redirect to quarantine server, a quarantine server must be configured first. Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC redirect:

```
DES-3528:5#enable jwac redirect
Command: enable jwac redirect

Success.

DES-3528:5#
```

disable jwac redirect

Purpose	Used to disable JWAC redirect function.
Syntax	disable jwac redirect
Description	This command only allows an unauthenticated host access to the quarantine server and the JWAC login page, all other web access will be denied.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC redirect:

```
DES-3528:5#disable jwac redirect
Command: disable jwac redirect

Success.

DES-3528:5#
```

enable jwac forcible_logout

Purpose	Used to enable JWAC Forcible Logout function.
Syntax	enable jwac forcible_logout
Description	This command allows a Ping packet with TTL=1 from an authenticated host to be regarded as a logout request by the JWAC enabled switch. As a result, the host will be moved back to an unauthenticated state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC forcible_logout:

```
DES-3528:5#enable jwac forcible_logout
Command: enable jwac forcible_logout

Success.

DES-3528:5#
```

disable jwac forcible_logout

Purpose	Used to disable JWAC forcible logout function.
Syntax	disable jwac forcible_logout
Description	This command is used to disable JWAC forcible logout function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC forcible_logout:

```
DES-3528:5#disable jwac forcible_logout
Command: disable jwac forcible_logout

Success.

DES-3528:5#
```

enable jwac udp filtering function

Purpose	Used to enable JWAC UDP filtering function.
Syntax	enable jwac udp_filtering
Description	This command is used to drop all UDP and ICMP packets, except DHCP and DNS packets, from unauthenticated hosts.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC udp_filtering:

```
DES-3528:5#enable jwac udp_filtering
Command: enable jwac udp_filtering

Success.

DES-3528:5#
```

disable jwac udp filtering function

Purpose	Used to disable JWAC UDP filtering function.
Syntax	disable jwac udp_filtering
Description	This command is used to disable JWAC UDP filtering function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC udp_filtering:

```
DES-3528:5#disable jwac udp_filtering
Command: disable jwac udp_filtering

Success.

DES-3528:5#
```

enable jwac quarantine_server_monitor

Purpose	Used to enable JWAC quarantine server monitor.
Syntax	enable jwac quarantine_server_monitor
Description	This command is for the JWAC switch to monitor the quarantine server ensuring that the server is okay. If the Switch does not detect any quarantine server, it will redirect all unauthenticated HTTP accesses to the JWAC Login Page when the redirect is enabled and the destination is configured as quarantine server.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC quarantine server monitor:

```
DES-3528:5#enable jwac quarantine_server_monitor
Command: enable jwac quarantine_server_monitor

Success.

DES-3528:5#
```


disable jwac quarantine_server_monitor

Purpose	Used to disable JWAC quarantine server monitor.
Syntax	disable jwac quarantine_server_monitor
Description	This command is used to disable JWAC quarantine server monitor.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC quarantine server monitor:

```
DES-3528:5#disable jwac quarantine_server_monitor
Command: disable jwac quarantine_server_monitor

Success.

DES-3528:5
```

config jwac quarantine_server_error_timeout

Purpose	Used to set Quarantine Server error timeout.
Syntax	config jwac quarantine_server_error_timeout <sec 5-300>
Description	When the Quarantine Server monitor is enabled, the JWAC Switch will periodically check if the Quarantine works okay. If the Switch does not receive any response from Quarantine Server during the configured error timeout, the Switch then regards it as not working properly.
Parameters	<sec 5-300> – To specify the error timeout interval
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC quarantine server error timeout:

```
DES-3528:5#config jwac quarantine_server_error_timeout 60
Command: config jwac quarantine_server_error_timeout 60

Success.

DES-3528:5#
```

config jwac redirect

Purpose	Used to configure redirect destination and delay time before an unauthenticated host is redirected to the Quarantine Server or the JWAC login web page.
Syntax	config jwac redirect {destination [quarantine_server jwac_login_page] delay_time <value 0-10>}(1)
Description	This command allows you to configure redirect destination and delay time before an unauthenticated host is redirected to the Quarantine Server or the JWAC login web page. The unit of delay time is seconds. 0 means no delaying the redirect.
Parameters	<i>destination</i> – To specify the destination which the unauthenticated host will be redirected to. <i>delay_time</i> – To specify the time interval after which the unauthenticated host will be redirected.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC redirect:

```
DES-3528:5#config jwac redirect destination jwac_login_page delay_time 5
Command: config jwac redirect_ destination jwac_login_page delay_time 5

Success.

DES-3528:5#
```

config jwac virtual_ip

Purpose	Used to configure JWAC virtual IP address used to accept authentication requests from an unauthenticated host.
Syntax	config jwac virtual_ip <ipaddr>
Description	The virtual IP of JWAC is used to accept authentication requests from unauthenticated hosts. Only requests sent to this IP will get a correct response. This IP does not respond to ARP requests or ICMP packets! Do not set this IP as the same subnet of the client PC and do not set its IP to the same as another device, otherwise the client PC cannot access the device.
Parameters	<ipaddr> – To specify the IP address of the virtual IP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC virtual IP:

```
DES-3528:5#config jwac virtual_ip 1.1.1.1
Command: config jwac virtual_ip 1.1.1.1

Success.

DES-3528:5#
```

config jwac quarantine_server_url

Purpose	Used to configure JWAC Quarantine Server URL
Syntax	config jwac quarantine_server_url <string 128>
Description	This command allows you to configure the URL of the Quarantine Server. If the redirect is enabled and the redirect destination is the Quarantine Server, when an HTTP request from unauthenticated host not to the Quarantine Server reaches the JWAC Switch, the Switch will handle this HTTP packet and send back a message to the host to make it access the Quarantine Server with the configured URL. When the PC connects to the specified URL, the quarantine server will request the PC user to input the user name and password to do authentication.
Parameters	<string 128> – To specify the entire URL of authentication page on Quarantine Server
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC quarantine server URL:

```
DES-3528:5#config jwac quarantine_server_url http://10.90.90.88/authpage.html
Command: config jwac quarantine_server_url http://10.90.90.88/authpage.html

Success.

DES-3528:5#
```



NOTE: If the quarantine server is linked to the JWAC enabled port on the switch, it must be added to the static FDB correctly before it can work properly.

config jwac clear_quarantine_server_url

Purpose	Used to clear Quarantine Server configuration.
Syntax	config jwac clear_quarantine_server_url
Description	This command will clear Quarantine Server configuration
Parameters	None.
Restrictions	When JWAC is enabled and the redirect destination is the Quarantine Server, the Quarantine Server cannot be cleared. Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC clear quarantine server URL:

```
DES-3528:5#config jwac clear_quarantine_server_url
Command: config jwac clear_quarantine_server_url

Success.

DES-3528:5#
```

config jwac update_server

Purpose	Used to configure the servers that PC may need to connect to in order to complete the JWAC authentication
Syntax	config jwac update_server [add delete] ipaddress <network_address>
Description	<p>This command allows you to add or delete server network addresses to which the traffic from unauthenticated client hosts will not be blocked by the JWAC Switch.</p> <p>Any servers the ActiveX needs to access to accomplish the authentication before the client passes the authentication should be added to the Switch with its IP address. For example, the client may need to access update.microsoft.com or some sites of the Anti-Virus software companies to check whether the OS or Anti-Virus software of the client is up-to-date; and so IP addresses of update.microsoft.com and of Anti-Virus software companies are needed to be added to the Switch.</p>
Parameters	<p><i>add</i> – To add a network address to which the traffic will not be blocked You can add five network addresses at the most</p> <p><i>delete</i> – To delete a network address to which the traffic will not be blocked</p> <p><i>ipaddress</i> – To specify the network address to add or delete To set a specific IP address, please use the format x.x.x.x/32</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC update server:

```
DES-3528:5#config jwac other_server add ipaddress 10.90.90.109/24
```

```
Command: config jwac other_server add ipaddress 10.90.90.109/24
```

```
Warning: the real added update server is 10.90.90.0/24
```

```
Success.
```

```
DES-3528:5#
```



NOTE: If the update server is linked to the JWAC enabled port on the switch, it must be added to the static FDB correctly before it can work properly.

config jwac switch_http_port

Purpose	Used to configure the TCP port which the JWAC Switch listens to.
Syntax	config jwac switch_http_port < tcp_port_number 1-65535> {[http https]}
Description	This command allows you to configure the TCP port which the JWAC Switch listens to. This port number is used in the second stage of the authentication. PC user will connect the page on the switch to input the user name and password. If not specified, the default port number is 80. If no protocol specified, the protocol is HTTP.
Parameters	<i>< tcp_port_number 1-65535></i> – A TCP port which the JWAC Switch listens to and uses to finish the authenticating process. <i>http</i> – To specify the JWAC runs HTTP protocol on this TCP port <i>https</i> – To specify the JWAC runs HTTPS protocol on this TCP port
Restrictions	The HTTP cannot run at TCP port 443, and the HTTPS cannot run at TCP port 80. Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC switch_http_port:

```
DES-3528:5#config jwac switch_http_port 8888 http
Command: config jwac switch_http_port 8888 http

Success.

DES-3528:5#
```

config jwac ports

Purpose	Used to configure port state of JWAC.
Syntax	config jwac ports [<portlist> all] {state [enable disable] max_authenticating_host <value 0 - n> aging_time [infinite <min 1 - 1440>] idle_time [infinite <min 1 - 1440>] block_time [<sec 0 - 300>] auth_mode [host_based port_based] }(1)
Description	This command allows you to configure port state of JWAC. The default value of <i>max_authenticating_host</i> is 50. The default value of <i>aging_time</i> is 1440 minutes. The default value of <i>idle_time</i> is infinite. The default value of <i>block_time</i> is 0 seconds.
Parameters	<portlist> – A port range to set the JWAC state. all – All the Switch ports' JWAC state is to be configured. state - To specify the port state of JWAC. <i>max_authenticating_host</i> – Max number of host process authentication on each port at the same time. The max authenticating hosts depends on a specific project. <i>aging_time</i> – A time period during which an authenticated host will keep an authenticated state. “infinite” indicates never to age out the authenticated host on the port <i>idle_time</i> – If there is no traffic during <i>idle_time</i> , the host will be moved back to unauthenticated state “infinite” indicates never to check the idle state of the authenticated host on the port. <i>block_time</i> – If a host fail to pass the authentication, it will be blocked for a period specified by <i>block_time</i> .
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC ports:

```
DES-3528:5#config jwac port 1-9 state enable
Command: config jwac port 1-9 state enable

Success.

DES-3528:5#
```

config jwac radius_protocol

Purpose	Used to configure radius protocol used by JWAC.
Syntax	config jwac radius_protocol [local pap chap ms_chap ms_chapv2 eap_md5]
Description	This command allows you to specify the RADIUS protocol used by JWAC to complete RADIUS authentication.
Parameters	<p><i>local</i> – JWAC Switch uses local user DB to complete the authentication</p> <p><i>pap</i> – JWAC Switch uses PAP to communicate with the RADIUS server.</p> <p><i>chap</i> – JWAC Switch uses CHAP to communicate with the RADIUS server.</p> <p><i>ms_chap</i> – JWAC Switch uses MS-CHAP to communicate with the RADIUS server.</p> <p><i>ms_chapv2</i> – JWAC Switch uses MS-CHAPv2 to communicate with RADIUS server.</p> <p><i>eap_md5</i> – JWAC Switch uses EAP MD5 to communicate with the RADIUS server.</p>
Restrictions	<p>JWAC share other RADIUS configuration with 802.1X, when using this command to set the RADIUS protocol, you must make sure the RADIUS server added by the config radius command supports the protocol.</p> <p>Only Administrator and Operator-level users can issue this command.</p>

Example usage:

To configure JWAC radius_protocol:

```
DES-3528:5#config jwac radius_protocol ms_chapv2
Command: config jwac radius_protocol ms_chapv2

Success.

DES-3528:5#
```

create jwac user

Purpose	Used to create JWAC user into local DB.
Syntax	create jwac user <username 15> {vlan <vlanid 1-4094>}
Description	This command creates JWAC users into the local DB. When “local” is chosen during configuring jwac RADIUS protocol, the local DB will be used.
Parameters	<p><i><username 15></i> – The user name to be created. The max length of the username is 15 characters</p> <p><i><vlanid 1-4094></i> – Target VLAN ID for authenticated host which uses this user account to pass authentication.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a JWAC user:

```
DES-3528:5#create jwac user twatanabe
Command: create jwac user twatanabe

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

DES-3528:5#
```

config jwac user

Purpose	Used to update local user DB.
Syntax	config jwac user <username 15> {vlan <vlanid 1-4094>}
Description	This command updates the local user DB. Only the created user can be configured.
Parameters	<p><i><username 15></i> – The user name to be created. The max length of the username is 15 characters.</p> <p><i><vlanid 1-4094></i> – Target VLAN ID for authenticated host which uses this user account to pass authentication.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a JWAC user:

```
DES-3528:5#config jwac user twatanabe vlan 3
Command: config jwac user twatanabe vlan 3

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

DES-3528:5#
```

delete jwac user

Purpose	Used to delete JWAC user from the local DB.
Syntax	delete jwac [user <username 15> all_users]
Description	This command deletes JWAC users from the local DB.
Parameters	<p><i>user</i> – To specify the user name to be deleted</p> <p><i>all_user</i> – All user accouts in local DB will be deleted.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a JWAC user:

```
DES-3528:5#delete jwac user twatanabe
Command: delete jwac user twatanabe

Success.

DES-3528:5#
```


show jwac user

Purpose	Used to show JWAC user in the local DB.
Syntax	show jwac user
Description	This command displays JWAC users in the local DB.
Parameters	None
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show a JWAC user:

```
DES-3528:5#show jwac user
Command: show jwac user

Username          Password          VID
-----          -
twatanabe         123              2

Total Entries:1

DES-3528:5#
```

clear jwac auth_state

Purpose	Used to delete host on JWAC enabled ports
Syntax	clear jwac auth_state [ports [all <portlist>] {authenticated authenticating blocked} mac_addr <macaddr>]
Description	This command allows you to delete JWAC host.
Parameters	<p><i>ports</i> – To specify the port range to delete host on them.</p> <p><i>authenticated</i> – To specify the state of host to delete.</p> <p><i>authenticating</i> – To specify the state of host to delete.</p> <p><i>blocked</i> – To specify the state of host to delete.</p> <p><i><macaddr></i> – To delete a specified host with this MAC.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a JWAC host:

```
DES-3528:5# clear jwac auth_state ports all blocked
Command: clear jwac auth_state ports all blocked

Success.

DES-3528:5#
```

show jwac

Purpose	Used to display the configuration of JWAC
Syntax	show jwac
Description	This command allows you to show all the configuration of JWAC.
Parameters	None
Restrictions	None

Example usage:

To display JWAC configuration:

```
DES-3528:5#show jwac
Command: show jwac

State                : Disabled
Enabled Ports        :
Virtual IP           : 0.0.0.0
Switch HTTP Port     : 80 (HTTP)
UDP Filtering        : Enabled
Forcible Logout      : Enabled
Redirect State       : Enabled
Redirect Delay Time  : 1 Seconds
Redirect Destination : Quarantine Server
Quarantine Server    :
Q-Server Monitor     : Disabled
Q-Srv Error Timeout  : 30 Seconds
RADIUS Auth-Protocol : PAP
Authentication Failover : Disabled
RADIUS Authorization : Enabled
Local Authorization  : Enabled
Update Server        :172.18.202.1/32
                    :172.18.202.0/24
                    :10.1.1.0/24

DES-3528:5#
```

show jwac auth_state ports

Purpose	Used to display information of JWAC client host
Syntax	show jwac auth_state ports {<portlist>}
Description	<p>This command allows you to show the information of JWAC client host.</p> <p>If port 1 is in host-based mode:</p> <p>(1) mac 00-00-00-00-00-01 is authenticated without VLAN assigned (may be the specified target VLAN does not exist or the target VLAN has not been specified), the ID of RX VLAN will be displayed (RX VLAN ID is 4004 in this example).</p> <p>(2) mac 00-00-00-00-00-02 is authenticated with target VLAN assigned, the ID of target VLAN will be displayed (target VLAN ID is 1234 in this example)</p> <p>(3) mac 00-00-00-00-00-03 failed to pass authentication, the VID field will be shown as “-” indicating that packets with SA 00-00-00-00-00-03 will be dropped no matter which VLAN these packets are from.</p> <p>(4) mac 00-00-00-00-00-04 attempts to start authentication, the VID field will be shown as “-” until authentication completed.</p> <p>If port 2 is in port-based mode:</p> <p>(1) mac 00-00-00-00-00-10 is the mac which made port 2 pass authentication, mac address with “(P)” in the end indicates that this authentication is from a port in port-based mode.</p> <p>If port 3 is in port-based mode:</p> <p>(1) mac 00-00-00-00-00-20 attempts to start authentication, mac address with “(P)” in the end indicates the port-based mode authentication.</p> <p>(2) mac 00-00-00-00-00-21 failed to pass authentication, mac address with “(P)” in the end indicates the port-based mode authentication.</p> <p>NOTE : In port-based mode, the VLAN ID field is displayed in the same way as host-based mode</p>
Parameters	<i>port</i> – A port range to show the information of client host.
Restrictions	None.

Example usage:

To display a JWAC host.

```
DES-3528:5#show jwac auth_state ports 5
Command: show jwac auth_state ports 5
```

Port	MAC Address	State	VLAN ID	Assigned	Aging Time/ Priority	Idle Time Block Time
5	00-05-5D-10-5A-6F	Authenticating	-	-	4	-

```
Total Authenticating Hosts : 1
Total Authenticated Hosts : 0
Total Blocked Hosts : 0
DES-3528:5#
```

show jwac ports

Purpose	Used to display port configuration of JWAC
Syntax	show jwac ports <portlist>
Description	The show jwac port command allows you to display port configuration of JWAC
Parameters	<portlist> – To specify a port range to show the configuration of JWAC
Restrictions	None.

Example usage:

To display JWAC ports.

```
DES-3528:5#show jwac ports 1-3
Command: show jwac ports 1-3
```

Port	State	Aging Time (Minutes)	Idle Time (Minutes)	Block Time (Seconds)	Auth Mode	Max Hosts
1	Disabled	1440	Infinite	60	Host_based	50
2	Disabled	1440	Infinite	60	Host_based	50
3	Disabled	1440	Infinite	60	Host_based	50

```
DES-3528:5#
```

config jwac authentication_page element

Purpose	Used to customize the authentication page.
Syntax	config jwac authentication_page element [japanese english] [default page_title <desc 128> login_window_title <desc 32> user_name_title <desc 16> password_title <desc 16> logout_window_title <desc 32>]
Description	This command allows the administrator to customize the JWAC authentication page.
Parameters	<p><i>japanese</i> – Specifies that the page will change to Japanese.</p> <p><i>english</i> – Specifies that the page will change to English.</p> <p><i>default</i> – Specifies to reset the page element back to default.</p> <p><i>page_title</i> – Specifies the title of the authentication page.</p> <p><i>login_window_title</i> – The login window title of the authentication page.</p> <p><i>user_name_title</i> – Specifies the user name title of the authentication page.</p> <p><i>password_title</i> – Specifies the password title of the authentication page.</p> <p><i>logout_window_title</i> – The logout window title mapping of the authentication page.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure authentication page.

```
DES-3528:5#config jwac authentication_page element japanese default
Command: config jwac authentication_page element japanese default
```

```
Success.
```

```
DES-3528:5#
```

config jwac auth_failover

Purpose	Used to enable or disable jwac auth_failover
Syntax	config jwac auth_failover [enable disable]
Description	This command allows the administrator to enable or disable jwac auth_failover. When the authentication failover is disabled and Radius servers are unreachable, the authentication will fail. When the authentication failover is enabled and Radius servers authentication are unreachable, the local database will be used to do the authentication. By default, the state is disabled.
Parameters	<i>enable</i> – Enable jwac auth_failover. <i>disable</i> – Disable jwac auth_failover.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable jwac auth_failover

```
DES-3528:5#config jwac auth_failover enable
Command: config jwac auth_failover enable

Success.

DES-3528:5#
```

config jwac authorization network

Purpose	Used to enable or disable the accepting of authorized configuration.
Syntax	config jwac authorization network {radius [enable disable] local[enable disable]}(1)
Description	This command allows the administrator to configure authorization network for JWAC. When the authorization is enabled for JWAC's radius, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. When the authorization is enabled for JWAC's local, the authorized data assigned by the local database will be accepted.
Parameters	<i>radius</i> –If specified to enable, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. The default state is enabled. <i>local</i> –If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the accepting of authorized configuration:

```
DES-3528:5#config jwac authorization network radius enable
Command: config jwac authorization network radius enable

Success.

DES-3528:5#
```

config jwac authenticate_page

Purpose	Used to choose authenticate page.
Syntax	config jwac authenticate_page [Japanese english]
Description	This command allows administrator to decide which authenticate page to be used.
Parameters	<i>japanese</i> – Choose the Japanese page <i>english</i> – Choose the english page, the default page is english.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To choose Japanese authenticate page.

```
DES-3528:5#config jwac authenticate_page japanese
Command: config jwac authenticate_page japanese

Success.

DES-3528:5#
```

show jwac authenticate_page element

Purpose	Used to show the element mapping of the customize authenticate page.
Syntax	show jwac authenticate_page element
Description	This command can display the element of the customize authenticate page.
Parameters	None
Restrictions	None

Example usage:

To display element of authenticate page.

```
DES-3528:5#show jwac authenticate_page element
```

```
Command: show jwac authenticate_page element
```

```
Current Page : Japanese Version
```

```
English page element
```

```
-----  
Page Title           :  
Login Window Title  : Authentication Login  
User Name Title     : User Name  
Password Title      : Password  
Login Out Window Title : Logout from the network
```

```
Japanese page element
```

```
-----  
Page Title           :  
Login Window Title  : 社内 LAN 認証ログイン  
User Name Title     : ユーザ ID  
Password Title      : パスワード  
Login Out Window Title : 社内 LAN 認証ログアウト
```

```
DES-3528:5#
```

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 < 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}(1)] [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 }(1)] [enable disable]
config lldp ports	[<portlist> all] dot3_tlvs [{all} {mac_phy_configuration_status link aggregation power_via_mdi maximum_frame_size}(1)] [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 operation on the Switch.
Syntax	enable lldp
Description	This is a global control for the LLDP function. When this function is enabled, the switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per port LLDP setting. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. The default state for LLDP is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable LLDP:

```
DES-3528:5#enable enable lldp
Command: enable lldp

Success.

DES-3528:5#
```

disable lldp

Purpose	Used to disable LLDP operation on the Switch.
Syntax	disable lldp
Description	This command will stop the sending and receiving of LLDP advertisement packets on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable LLDP:

```
DES-3528:5#disable lldp
Command: disable lldp

Success.

DES-3528:5#
```

config lldp message_tx_interval

Purpose	Used to change the packet transmission interval.
Syntax	config lldp message_tx_interval <sec 5 – 32768>
Description	This interval controls how often active ports retransmit advertisements to their neighbors.
Parameters	<i>message_tx_interval</i> – Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The range is from 5 seconds to 32768 seconds. The default setting is 30 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To show the packet transmission interval:

```
DES-3528:5#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DES-3528:5#
```

config lldp message_tx_hold_multiplier

Purpose	Used to configure the message hold multiplier.
Syntax	config lldp message_tx_hold_multiplier < 2 - 10 >
Description	This command is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU. TheTTL 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	<i>Message_tx_hold_multiplier</i> – The range is from 2 to 10. The default setting is 4.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:


To change the multiplier value:

```
DES-3528:5#config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

DES-3528:5#
```

config lldp tx_delay

Purpose	Used to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The tx_delay defines the minimum interval between sending of LLDP messages due to constantly change 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	<i>tx_delay</i> – The range is from 1 second to 8192 seconds. The default setting is 2 seconds.
	 NOTE: txDelay should be less than or equal to 0.25 * msgTxInterval.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the delay interval:

```
DES-3528:5#config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DES-3528:5#
```

config lldp reinit_delay

Purpose	Change the minimum time of the reinitialization 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	<i>reinit_delay</i> – The range is from 1 second to 10 seconds. The default setting is 2 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To changes the re-initialization delay interval to five seconds:

```
DES-3528:5#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DES-3528:5#
```

config lldp notification_interval

Purpose	Used to configure the timer of the notification interval for sending notification to configured SNMP trap receiver(s).
Syntax	config lldp notification_interval <sec 5 – 3600 >
Description	This command is used to globally change the interval between successive LLDP change notifications generated by the switch.
Parameters	<i>notification_interval</i> – The range is from 5 seconds to 3600 seconds. The default setting is 5 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To change the notification interval to 10 seconds:

```
DES-3528:5#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DES-3528:5#
```

config lldp ports notification

Purpose	Used to configure each port for sending notification to configured SNMP trap receiver(s).
Syntax	config lldp ports [<portlist> all] notification [enable disable]
Description	This command is used to enable or disable each port for sending changes notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout, information update. And the changed type includes any data update /insert/remove.
Parameters	<i><portlist></i> – Use this parameter to define ports to be configured. <i>all</i> – Use this parameter to set all ports in the system. <i>notification</i> – Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.

config lldp ports notification

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

Example usage:

To change the SNMP notification state of ports 1 to 5 to enable:

```
DES-3528:5#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DES-3528:5#
```

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 This command is used 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
 <portlist> – Use this parameter to define ports to be configured.
 all – Use this parameter to set all ports in the system.
 admin_status – tx_only: Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices; rx_only: Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors; tx_and_rx: Configure the specified port(s) to both transmit and receive LLDP packets;
 disable: Disable LLDP packet transmit and receive on the specified port(s). The default per port state is tx_and_rx.

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

Example usage:

To configure ports 1 to 5 to transmit and receive:

```
DES-3528:5#config lldp ports 1-5 admin_status rx_and_tx
Command: config lldp ports 1-5 admin_status rx_and_tx

Success.

DES-3528:5#
```

config lldp ports mgt_addr

Purpose Used to enable or disable port(s) specified for advertising indicated management address instance.

Syntax `config lldp ports [<portlist> | all] mgt_addr [ipv4 <ipaddr>] [enable | disable]`

Description This command specifies 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
 <portlist> – Use this parameter to define ports to be configured.
 all – Use this parameter to set all ports in the system.
 ipv4 – The IP address of IPv4.

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

Usage Example:

To enable ports 1 to 2 to manage address entry:

```
DES-3528:5#config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable
Command: config config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable

Success.

DES-3528:5#
```

config lldp ports basic_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more 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 include four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory type cannot be disabled. There are also four data types which can be optionally selected. They are <i>port_description</i> , <i>system_name</i> , <i>system_description</i> , and <i>system_capability</i> .
Parameters	<p><i><portlist></i> – Use this parameter to define ports to be configured.</p> <p><i>all</i> – Use this parameter to set all ports in the system.</p> <p><i>port_description</i> – This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled.</p> <p><i>system_name</i> – This TLV optional data type indicates that LLDP agent should transmit 'System Name TLV'. The default state is disabled.</p> <p><i>system_description</i> – This TLV optional data type indicates that LLDP agent should transmit 'System Description TLV'. The default state is disabled.</p> <p><i>system_capabilities</i> – This TLV optional data type indicates that LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DES-3528:5#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DES-3528:5#
```

config lldp 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 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> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</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 disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the VLAN nameTLV from the outbound LLDP advertisements for all ports:

```
DES-3528:5#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DES-3528:5#
```

config lldp dot1_tlv_protocol_vid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_protocol_vid [vlan [all <vlan_name 32>] vlanid <vlanid_list>] [enable disable]
Description	This TLV optional data type indicates whether the corresponding Local System's port and protocol VLAN ID instance will be transmitted on the port. If a port is associated with multiple protocol VLANs, those enabled port and protocol VLAN IDs will be advertised.
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>dot1_tlv_protocol_vid – This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DES-3528:5#config lldp ports all dot1_tlv_protocol_vid vlnid 1-3 enable
Command: config lldp ports all dot1_tlv_protocol_vid vlnid 1-3 enable

Success.

DES-3528:5#
```

config lldp dot1_tlv_vlan_name

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_vlan_name [vlan [all <vlan_name 32>] vlanid <vlanid_list>] [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	<p><i><portlist></i> – Use this parameter to define ports to be configured.</p> <p><i>all</i> – Use this parameter to set all ports in the system.</p> <p><i>dot1_tlv_vlan_name</i> – 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 disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DES-3528:5#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-3528:5#
```

config lldp dot1_tlv_protocol_identity

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_protocol_identity [all {eapol lacp gvrp stp }(1)] [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 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><i><portlist></i> – Use this parameter to define ports to be configured.</p> <p><i>all</i> – Use this parameter to set all ports in the system.</p> <p><i>dot1_tlv_protocol_identity</i> – This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DES-3528:5#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DES-3528:5#
```

config lldp dot3_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.
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	<p><i><portlist></i> – Use this parameter to define ports to be configured.</p> <p><i>all</i> – Use this parameter to set all ports in the system.</p> <p><i>mac_phy_configuration_status</i> – 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 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.</p> <p><i>link_aggregation</i> – 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.</p> <p><i>power_via_mdi</i> – This TLV optional data type indicates that the 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. Note: Not supported in the current release.</p> <p><i>maximum_frame_size</i> – This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV'. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DES-3528:5#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-3528:5#
```


config lldp forward_message

Purpose	Used to configure the forwarding of LLDPDU 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 LLDPDU packets will be forwarded. The default state is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure LLDP forward_message:

```
DES-3528:5#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DES-3528:5#
```

show lldp

Purpose	Used to display the Switch's general LLDP configuration status.
Syntax	show lldp
Description	This command displays the switch's general LLDP configuration status.
Parameters	None.
Restrictions	None.

Usage Example:

To display the LLDP system level configuration status:

```
DES-3552:5#show lldp
Command: show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-80-C2-11-22-00
  System Name             :
  System Description      : Fast Ethernet Switch
  System Capabilities     : Repeater, Bridge

LLDP Configurations
  LLDP Status             : Disabled
  LLDP Forward Status     : Disabled
  Message Tx Interval    : 30
  Message Tx Hold Multiplier: 4
  ReInit Delay           : 2
  Tx Delay                : 2
  Notification Interval  : 5

DES-3552:5#
```

show lldp mgt_addr

Purpose	Used to display the LLDP management address information.
Syntax	show lldp mgt_addr {ipv4 <ipaddr>}
Description	This command displays the LLDP management address information.
Parameters	<i>ipv4</i> – The IP address of IPv4.
Restrictions	None.

Example usage:

To display management address information 1:

```
DES-3528:5#show lldp mgt_addr ipv4 10.24.73.21
Command: show lldp mgt_addr ipv4 10.24.73.21

Address 1
-----
Subtype           : IPv4
Address           : 10.24.73.21
IF type          : Unknown
OID               : 1.3.6.1.4.1.171.10.105.1
Advertising Ports :

DES-3528:5#
```

show lldp ports

Purpose	Used to display the LLDP per port configuration for advertisement options.
Syntax	show lldp ports {<portlist>}
Description	This command displays the LLDP per port configuration for advertisement options.
Parameters	<portlist> – Use this parameter to define ports to be configured.
Restrictions	None.

Example usage:

To display the LLDP per port TLV option configuration:

```
DES-3528:5#show lldp ports 1
Command: show lldp ports 1

Port ID                : 1
-----
Admin Status           : TX_and_RX
Notification Status    : Disabled
Advertised TLVs Option :
  Port Description      Disabled
  System Name           Disabled
  System Description    Disabled
  System Capabilities   Disabled
  Enabled Management Address
    (None)
  Port VLAN ID          Disabled
  Enabled Port_and_Protocol_VLAN_ID
    (None)
  Enabled VLAN Name     (None)
  Enabled Protocol_Identity
    (None)
  MAC/PHY Configuration/Status Disabled
  Link Aggregation      Disabled
  Maximum Frame Size    Disabled
```

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

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 displays the per-port information currently available for populating outbound LLDP advertisements.
Parameters	<p><i><portlist></i> – Use this parameter to define ports to be configured.</p> <p><i>brief</i> – Display the information in brief mode.</p> <p><i>normal</i> – Display the information in normal mode. This is the default display mode.</p> <p><i>detailed</i> – Display the information in detailed mode.</p>
Restrictions	None.

Usage Example:

To display outbound LLDP advertisements for port 1-2:

```

DES-3528:5#show lldp local_ports 1-2
Command: show lldp local_ports 1-2

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 : 0
MAC/PHY Configuration/Status : (See Detail)
Link Aggregation         : (See Detail)
Maximum Frame Size       : 1536

Port ID : 2
-----
Port ID Subtype           : Local
Port ID                   : 1/1
Port Description          : RMON Port 1 on Unit 1
Port PVID                 : 1
Management Address Count  : 1

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

```

show lldp remote_ports

Purpose	Used to display the information learned from the neighbor.
Syntax	show lldp remote_ports {<portlist>} {mode [brief normal detailed]}
Description	This command displays the information learned from the neighbor parameters. Due to a memory limitation, only 32 VLAN Name entries and 10 Management Address entries can be received.
Parameters	<p><i><portlist></i> – Use this parameter to define ports to be configured.</p> <p><i>mode</i> – Choose from three options:</p> <p><i>brief</i> – Display the information in brief mode.</p> <p><i>normal</i> – Display the information in normal mode. This is the default display mode.</p> <p><i>detailed</i> – Display the information in detailed mode.</p>
Restrictions	None.

Example usage:

To display remote table in brief mode:

```

DES-3528:5#show lldp remote_ports 1-2 mode brief
Command: show lldp remote_ports 1-2 mode brief

Port ID: 1
-----
Remote Entities Count   : 1
Entity 1
  Chassis ID Subtype    : MAC Address
  Chassis ID            : 00-01-0-2-03-04-01
  Port ID Subtype       : Local
  Port ID               : 1/3
  Port Description      : RMON Port 1 on Unit 3

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

```

show lldp statistics

Purpose	Used to display the system LLDP statistics information.
Syntax	show lldp statistics
Description	This command displays an overview of neighbor detection activity on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display global statistics information:

```
DES-3528:5#show lldp statistics
Command: show lldp statistics

Last Change Time           : 1705
Number of Table Insert     : 0
Number of Table Delete     : 0
Number of Table Drop       : 0
Number of Table Ageout     : 0

DES-3528:5#
```

show lldp statistics ports

Purpose	Used to display the ports LLDP statistics information.
Syntax	show lldp statistics ports{<portlist>}
Description	This command displays per-port LLDP statistics.
Parameters	<portlist> – Use this parameter to define ports to be configured. When portlist is not specified, information for all ports will be displayed.
Restrictions	None.

Usage Example:

To display statistics information of port 1:

```
DES-3528:5#show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
-----
LLDPStatsTxPortFramesTotal      : 0
LLDPStatsRxPortFramesDiscardedTotal : 0
LLDPStatsRxPortFramesErrors    : 0
LLDPStatsRxPortFramesTotal     : 0
LLDPStatsRxPortTLVsDiscardedTotal : 0
LLDPStatsRxPortTLVsUnrecognizedTotal : 0
LLDPStatsRxPortAgeoutsTotal    : 0

DES-3528:5#
```

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 inner_tpid	
config qinq ports	[<portlist> all] {role [uni nni] missdrop [enable disable] outer_tpid <hex 0x1 - 0xffff> use_inner_priority [enable disable] vlan_preservation [enable disable] add_inner_tag [<hex 0x1 - 0xffff> disable]} (1)
show qinq ports	{<portlist>}
config qinq inner_tpid	<hex 0x1 - 0xffff>
create vlan_translation ports	[<portlist> all] cvid <vidlist> [add replace] svid <vlanid 1-4094> {priority <value 0-7>}
delete vlan_translation ports	[<portlist> all] {cvid <vidlist>}
show vlan_translation	{ports <portlist> }

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

enable qinq

Purpose	Used to enable Q-in-Q mode.
Syntax	enable qinq
Description	<p>This command enables Q-in-Q mode.</p> <p>When enable Q-in-Q, all network port roles will be NNI port and their outer TPID will be set to 88a8. All existed static VLAN will run as SP-VLAN. 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, you shall enable GVRP manually. In Q-in-Q mode, SP-VLAN GVRP Address (01-80-C2-00-00-0D) will be used by GVRP protocol.</p> <p>The default setting of Q-in-Q is disabled</p>
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To enable Q-in-Q:

```
DES-3528:5#enable qinq
Command: enable qinq

Success.

DES-3528:5#
```

disable qinq

Purpose	Used to disable the Q-in-Q mode.
Syntax	disable qinq
Description	This command disables the Q-in-Q mode. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared. GVRP will disable. If you need to run GVRP on the switch, you shall enable GVRP manually. All existed SP-VLAN will run as static 1Q VLAN
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To disable Q-in-Q:

```
DES-3528:5#disable qinq
Command: disable qinq

Success.

DES-3528:5#
```

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
Parameters	None
Restrictions	None.

Example usage

To show global Q-in-Q status:

```
DES-3528:5#show qinq
Commands: show qinq

QinQ Status: Enabled

DES-3528:5#
```

configure qinq ports

Purpose	Used to configure Q-in-Q port.
Syntax	config qinq ports [<portlist> all] {role [uni nni] missdrop [enable disable] outer_tpid <hex 0x1 - 0xffff> use_inner_priority [enable disable] vlan_preservation [enable disable] add_inner_tag [<hex 0x1 - 0xffff> disable]}(1)
Description	<p>This command is used to configure the Q-in-Q VLAN mode for ports, include:</p> <p>port role in double tag VLAN mode, enable/disable SP-VLAN assignment miss drop, port outer TPID, use inner priority, and enable/disable add inner tag.</p> <p>If missdrop is enabled, the packet that does not match any assignment rule in the Q-in-Q profile will be dropped. If disabled, then the packet will be assigned to the PVID of the received port.</p> <p>This setting will not be effective when Q-in-Q mode is disabled.</p>
Parameters	<p><i>portlist</i> – A range of ports to configure.</p> <p><i>role</i> – Port role in Q-in-Q mode, it can be either UNI port or NNI port.</p> <ul style="list-style-type: none"> UNI – User-to-Network Interface specifies that communication between the specified user and a specified network will occur. NNI – Network-to-Network Interface specifies that communication between two specified networks will occur. <p><i>missdrop</i> – enable/disable C-VLAN based SP-VLAN assignment miss drop.</p> <p><i>outer_tpid</i> – Allows the interoperability with devices on a public network by specifying ports.</p> <p><i>use_inner_priority</i> – Specifies whether to use the priority in the C-VLAN tag as the priority in the SP-VLAN tag.</p> <p><i>vlan_preservation</i> – Specifies to enable or disable VLAN preservation.</p> <p><i>add_inner_tag</i> - Specifies whether to add inner tag for ingress untagged packets. If set, the inner tag will be added for the ingress untagged packets and thus the packets egress to the NNI port will be double tagged. If disable, only s-tag will be added for ingress untagged packets.</p>
Restrictions	Only Administrator and Operator-level users can issue this command. You must be in the Q-in-Q mode.

Example usage

To config port list 1-4 as NNI port, set outer TPID to 0x88a8:

```
DES-3528:5#config qinq ports 1-4 role nni outer_tpid 0x88a8
Command: config qinq ports 1-4 role nni outer_tpid 0x88a8

Success.

DES-3528:5#
```

show qinq ports

Purpose	Used to show global Q-in-Q and port's Q-in-Q mode status.
Syntax	show qinq ports <portlist>
Description	<p>This command is used to show the Q-in-Q configuration for a port, include:</p> <p>port role in Q-in-Q mode, enable/disable to drop the SP-VLAN assignment miss packet, port outer TPID, use inner priority, and enable/disable add inner tag.</p>
Parameters	<p><i>portlist</i> – Specifies a range of ports to be displayed.</p> <p>If no parameter specified, system will display all ports information.</p>
Restrictions	None.

Example usage

To show double tagging mode for ports 1-4 of unit 1:

```
DES-3528:5#show qinq ports 1:1-1:4
Command: show qinq ports 1:1-1:4
```

Port	Role	Missdrop	Outer TPID	Use Inner Priority	Add Inner Tag	Prev
1:1	NNI	Disabled	0x88A8	Disabled	Disabled	On
1:2	NNI	Disabled	0x88A8	Disabled	Disabled	On
1:3	NNI	Disabled	0x88A8	Disabled	Disabled	On
1:4	NNI	Disabled	0x88A8	Disabled	Disabled	On

```
DES-3528:5#
```

config qinq inner_tpid

Purpose Used to configure the system's inner TPID.

Syntax `config qinq inner_tpid <hex 0x1 - 0xffff>`

Description The command is used to configure the inner TPID of the system. The inner TPID is used to decide whether the ingress packet is c-tagged. Inner tag TPID is per system configurable. This command is for projects that support per system TPID configuration. For projects that support per port TPID configuration, the config qinq ports inner_tpid command should be supported.

Parameters None.

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

Example usage

To configure the inner TPID in the system to 0x9100:

```
DES-3528:5# config inner_TPID 0x9100
```

Success.

```
DES-3528:5#
```

create vlan_translation ports

Purpose	Used to create VLAN translation rule.
Syntax	create vlan_translation ports [<portlist> all] cvid <vidlist> [add replace] svid <vlanid 1-4094> {priority <value 0-7>}
Description	<p>This command can be used to add translation relationship between C-VLAN and SP-VLAN. On ingress at UNI port, the C-VLAN tagged packets will be translated to SP-VLAN tagged packets by adding or replacing according the configured rule. On egress at this port, the SP-VLAN tag will be recovered to C-VLAN tag or be striped.</p> <p>The priority will be the priority in the SP-VLAN tag if the use_inner_priority flag is disabled for the receipt port.</p> <p>This configuration is only effective for an UNI port.</p> <p>This setting will not be effective when Q-in-Q mode is disabled.</p> <p>Note that if the action of the rule replaces C-VLAN tag, the relationship between C-VLAN and S-VLAN on the port shall be one-to-one mapping. Multiple C-VLAN map to one S-VLAN on a port is not supported, users shall take care of this while configuring the rules.</p>
Parameters	<p><i>portlist</i> – A range of ports under Q-in-Q rules which assign the SP-VLAN tag based on the C-VLAN tag for received C-VLAN tagged packets on these ports.</p> <p><i>cvid</i> – C-VLAN ID to match.</p> <p><i>add</i> – The action indicates to add a tag for the assigned SP-VLAN before the C-VLAN tag.</p> <p><i>replace</i> – The action indicates to replace the C-VLAN tag with the SP VLAN</p> <p><i>svid</i> – SP-VLAN ID.</p> <p><i>priority</i> – The priority of the s-tag.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To create vlan translation rule which assign to add SP-VLAN 100 to C-VLAN 1-10 on ports 1-4 and the priority is 4:

```
DES-3528:5#create vlan_translation ports 1-4 cvid 10 add svid 100 priority 4
Command: create vlan_translation ports 1-4 cvid 10 add svid 100 priority 4
```

Success.

```
DES-3528:5#
```

delete vlan_translation ports

Purpose	Used to delete pre-created VLAN translation rules.
Syntax	delete vlan_translation ports [<portlist> all] {cvid <vidlist>}
Description	The command is used to delete pre-created VLAN translation rules.
Parameters	<p><i>ports</i> – A range of ports which the rule will be deleted.</p> <p><i>cvid</i> – Specify C-VLAN range which the rules will be deleted. If no specify the parameter, all rules on the specified ports will be deleted.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To delete vlan translation rule on ports 1-4:

```
DES-3528:5#delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DES-3528:5#
```

show vlan_translation

Purpose	Used to show pre-created C-VLAN based SP-VLAN assignment rules.
Syntax	show vlan_translation {ports <portlist>}
Description	The command is used to show pre-created C-VLAN based SP-VLAN assignment rules.
Parameters	<i>ports</i> – A range of ports which the rules will be displayed. If no parameters specified, all rules will be displayed.
Restrictions	None.

Example usage

To show vlan_translation rules in the system:

```
DES-3528:5#show vlan_translation
Commands: show vlan_translation

Port          CVID      SPVID      Action      Priority
-----
1             10        100        Add         4
1             20        100        Add         5
1             30        200        Add         6
2             10        100        Add         7
2             20        100        Add         1
Total Entries: 5

DES-3528:5#
```

RSPAN COMMANDS

The Remote Switched Port Analyzer (RSPAN) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable rspan	
disable rspan	
create rspan vlan	[vlan_name <vlan_name> vlan_id <value 1-4094>]
delete rspan vlan	[vlan_name <vlan_name> vlan_id <value 1-4094>]
config rspan vlan	[vlan_name <vlan_name> vlan_id <vlanid 1-4094>] [redirect [add delete] port <port> source {[add delete] ports <portlist> [rx tx both]}]
show rspan	{[vlan_name <vlan_name> vlan_id <vlanid 1-4094>]}

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

enable rspan

Purpose Used to enable RSPAN.

Syntax **enable rspan**

Description This command controls the RSPAN function. The purpose of RSPAN function is to mirror the packets to the remote switch. The packet travels from the switch where the monitored packet is received, through an intermediate switch, then to the switch where the sniffer is attached. The first switch is also named the source switch. To make the RSPAN work, for the source switch, the RSPAN VLAN source setting must be configured. For the intermediate and the last switch, the RSPAN VLAN redirect setting must be configured.



NOTE: RSPAN VLAN mirroring only works when RSPAN is enabled, an RSPAN VLAN has been configured with source ports, and mirror is enabled. RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

Parameters None.

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

Example usage:

To enable RSPAN:

```
DES-3528:5#enable rspan
```

```
Command: enable rspan
```

```
Success.
```

```
DES-3528:5#
```

disable rspan

Purpose	Used to disable RSPAN.
Syntax	disable rspan
Description	This command controls the RSPAN function
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable RSPAN:

```
DES-3528:5#disable rspan
Command: disable rspan

Success.

DES-3528:5#
```

create rspan vlan

Purpose	Used to create an RSPAN VLAN.
Syntax	create rspan vlan [vlan_name <vlan_name> vlan_id <value 1-4094>]
Description	This command is used to create the RSPAN VLAN. Up to 16 RSPAN VLANs can be created.
Parameters	<i>vlan_name</i> – Create the RSPAN VLAN by VLAN name. <i>vlan_id</i> – Create the RSPAN VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a RSPAN VLAN:

```
DES-3528:5#create rspan vlan vlan_name v3
Command: create rspan vlan vlan_name v3

Success.

DES-3528:5#
```

delete rspan vlan

Purpose	Used to delete a RSPAN VLAN.
Syntax	delete rspan vlan [vlan_name <vlan_name> vlan_id <value 1-4094>]
Description	This command is used to delete RSPAN VLANs.
Parameters	<i>vlan_name</i> – Delete RSPAN VLAN by VLAN name. <i>vlan_id</i> – Delete RSPAN VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a RSPAN VLAN:



```
DES-3528:5#delete rspan vlan vlan_name v3
```

```
Command: delete rspan vlan vlan_name v3
```

Success.

```
DES-3528:5#
```

config rspan vlan

Purpose	Used by the source switch to configure the source setting for the RSPAN VLAN.
Syntax	config rspan vlan [vlan_name <vlan_name> vlan_id <vlanid 1-4094>] [redirect [add delete] port <port> source {[add delete] ports <portlist> [rx tx both]]]
Description	<p>This command configures the source and redirect setting for the RSPAN VLAN on the Switch. The output port of the RSPAN mirrored packet will use the same destination port as defined by the mirror command. The redirect command makes sure that the RSPAN VLAN packets can be egress to the redirect ports. In addition to this redirect command, the VLAN setting must be correctly configured to make the RSPAN VLAN work correctly. That is, for the intermediate switch, the redirect port must be a tagged member port of RSPAN VLAN. For the last switch, the redirect port must be either a tagged member port or an untagged member port of the RSPAN VLAN based on the users requirements. If untagged membership is specified, the RSPAN VLAN tag will be removed. The redirect function will only work when RSPAN is enabled. Multiple RSPAN VLANs can be configured with redirect settings at the same time.</p> <p> NOTE: If RSPAN is enabled, the packets mirrored to the destination port are always added with an RSPAN VLAN tag. If mirror is enabled but RSPAN is disabled, the packets mirrored to the destination port may be in tagged form or in untagged form.</p> <p> NOTE: Only one RSPAN VLAN can be configured with source settings.</p>
Parameters	<p><i>vlan</i> – Specify the RSPAN VLAN on the source switch.</p> <p><i>vlan_name</i> – Specify RSPAN VLAN by VLAN name.</p> <p><i>vlan_id</i> – Specify RSPAN VLAN by VLAN ID.</p> <p><i>redirect</i> – Specify output port for the RSPAN VLAN packets.</p> <p><i>source</i> – Specify the source settings for the RSPAN VLAN on the source switch.</p> <p><i>add</i> – Add source ports into the RSPAN source.</p> <p><i>delete</i> – Delete source ports from the RSPAN source.</p> <p><i>ports</i> – Specify source portlist to add to or delete from the RSPAN source.</p> <p><i>rx</i> – Only monitor ingress packets.</p> <p><i>tx</i> – Only monitor egress packets.</p> <p><i>both</i> – Monitor both ingress and egress packets.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the rx traffic of port 2 to port 5 mirrored and add vid tag 2 :

```
DES-3528:5#config rspan vlan vlan_name v3 source add ports 2-5 rx
```

```
Command: config rspan vlan vlan_name v3 source add ports 2-5 rx
```

Success.

```
DES-3528:5#
```

show rspan

Purpose	Used to display RSPAN configuration.
Syntax	show rspan {[vlan_name <vlan_name> vlan_id <vlanid 1-4094>]}
Description	This command displays the RSPAN configuration.
Parameters	<i>vlan_name</i> – Specify the RSPAN VLAN by VLAN name. <i>vlan_id</i> – Specify the RSPAN VLAN by VLAN ID.
Restrictions	None.

Example usage:

To display special setting:

```
DES-3528:5#show rspan vlan_id 63
```

```
Command: show rspan vlan_id 63
```

```
RSPAN : Enabled
```

```
RSPAN VLAN ID : 63
```

```
-----
```

```
Source Ports
```

```
RX          : 2-5
```

```
TX          : 2-5
```

```
Total RSPAN VLAN:1
```

```
DES-3528:5#
```

STATIC MAC-BASED VLAN COMMANDS

The Static 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> vlanid <vlanid 1-4094>]
delete mac_based_vlan	{mac_address <macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
show mac_based_vlan	{mac_address <macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094>]}

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> vlanid <vlanid 1-4094>]
Description	This command only needs to be supported by the model which supports MAC-based VLAN. The user can use this command to create a static MAC-based VLAN entry. When a MAC-based VLAN entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN regardless of the authentication function operated on this port. There is a global limitation of the maximum entries supported for the static MAC-based entry.
Parameters	<i>mac_address</i> – The MAC address. <i>vlan</i> – The VLAN to be associated with the MAC address. <i>vlanid</i> - Specifies the VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To create a MAC-based VLAN entry:

```
DES-3528:5#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-3528:5#
```


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> vlanid <vlanid 1-4094>]}
Description	This command is used to delete a database entry. If the MAC address and VLAN is not specified, all static entries associated with the port will be removed.
Parameters	<p><i>mac_address</i> – The MAC address.</p> <p><i>vlan</i> – The VLAN to be associated with the MAC address.</p> <p><i>vlanid</i> - Specifies the VLAN by VLAN ID.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To delete a static MAC-based VLAN entry:

```
DES-3528:5#delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: delete mac_based_vlan mac mac_address 00-00-00-00-00-01 vlan default

Success.

DES-3528:5#
```

show mac_based_vlan

Purpose	Used to show the static or dynamic MAC-based VLAN entry.
Syntax	show mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
Description	This command is used to display the static or dynamic MAC-Based VLAN entry.
Parameters	<p><i>mac</i> – The MAC address.</p> <p><i>vlan</i> – The VLAN to be associated with the MAC address.</p> <p><i>vlanid</i> - Specifies the VLAN by VLAN ID.</p>
Restrictions	None.

Example usage

To display the static or dynamic MAC-based VLAN entry:

```
DES-3528:5#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    200       Inactive    Static
00-80-c2-33-c3-45    300       Active      Mac_based Access Control
00-80-c2-33-c3-90    400       Active      802.1x
00-a2-44-17-32-98    500       Active      JWAC

Total Entries : 5

DES-3528:5#
```

SIMPLE RED COMMANDS

The Simple RED commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable sred	
disable sred	
config sred	[<portlist> all] [<class_id 0-7> all] { threshold {low <value 0-100> high<value 0-100>}(1) drop_rate {low<value 1-8> high<value 1-8>}(1) drop_green [enable disable]}(1)
show sred	{ <portlist>{ <class_id 0-7>}}
show sred drop_counter	{<portlist>}
config dscp trust	[<portlist> all] state [enable disable]
show dscp trust	{<portlist>}
config dscp map	[<portlist> all] [dscp_priority <dscp_list> to <priority 0-7> dscp_dscp <dscp_list> to <dscp 0-63> dscp_color <dscp_list> to [green red yellow]]
show dscp map	{ <portlist> } [dscp_priotity dscp_dscp dscp_color] {dscp <dscp_list>}
config 802.1p map	[<portlist> all] 1p_color [<priority_list> to [green red yellow]]
show 802.1p map 1p_color	{ <portlist>}

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

enable sred

Purpose	Used to enable the simple RED function.
Syntax	enable sred
Description	This command is used to enable the sRED function. By default, sRED is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To enable sred:

```
DES-3528:5#enable sred
Command: enable sred

Success.

DES-3528:5#
```

disable sred

Purpose	Used to disable the simple RED function.
Syntax	disable sred
Description	This command is used to disable the sRED function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage


To disable sred:

```
DES-3528:5#disable sred
Command: disable sred

Success.

DES-3528:5#
```

config sred

Purpose	Used to config the simple RED parameter.																
Syntax	config sred [<portlist> all] [<class_id 0-7> all] { threshold {low <value 0-100> high<value 0-100>}(1) drop_rate {low<value 1-8> high<value 1-8>}(1) drop_green [enable disable]}(1)																
Description	This command is used to onfigure sRED threshold per port or per port per queue.																
Parameters	<p><i>portlist</i> – A range of ports to config.</p> <p><i>class_id</i> – This specifies which of the 8 hardware CoS queues the config sred command will apply to.</p> <p><i>threshold</i> – low – low threshold that Specifies the percent of space utilized. By default, the value is 60. The range is 0 to 100.</p> <p>high – high threshold that Specifies the percent of queue space utilized. By default, the value is 80. The range is 0 to 100.</p> <p><i>drop_rate</i> – low – probabilistic drop rate if above the low threshold, By default, the value is 1.</p> <p>high – probabilistic drop rate if above the high threshold. By default, the value is 1.</p> <p><i>drop_green</i> – disable – probabilistic drop red colored packets if the queue depth is above the low threshold, and probabilistic drop yellow colored packets if the queue depth is above the high threshold. By default, if the option is not specified, the setting is disable.</p> <p>enable – probabilistic drop yellow and red colored packets if the queue depth is above the low threshold, and probabilistic drop green colored packets if the queue depth is above the high threshold.</p>																
	<p> NOTE: There are 8 drop rates:</p> <table border="1"> <tr><td>1</td><td>100%</td></tr> <tr><td>2</td><td>6.25%</td></tr> <tr><td>3</td><td>3.125%</td></tr> <tr><td>4</td><td>1.5625%</td></tr> <tr><td>5</td><td>0.78125%</td></tr> <tr><td>6</td><td>0.390625%</td></tr> <tr><td>7</td><td>0.1953125%</td></tr> <tr><td>8</td><td>0.09765625%</td></tr> </table>	1	100%	2	6.25%	3	3.125%	4	1.5625%	5	0.78125%	6	0.390625%	7	0.1953125%	8	0.09765625%
1	100%																
2	6.25%																
3	3.125%																
4	1.5625%																
5	0.78125%																
6	0.390625%																
7	0.1953125%																
8	0.09765625%																
Restrictions	Only Administrator and Operator-level users can issue this command.																

Example usage

To configure sred:

```
DES-3528:5#config sred all all threshold low 64 high 80 drop_rate low 8 high 8
drop_green disable
Command: config sred all all threshold low 64 high 80 drop_rate low 8 high 8
drop_green disable

Success.

DES-3528:5#
```

show sred

Purpose	Used to display the simple RED configure parameter.
Syntax	show sred { <portlist>{ <class_id 0-7>}}
Description	This command displays the current threshold(per port and per queue) parameters in use on the switch
Parameters	<i>portlist</i> – A range of ports to show. <i>class_id</i> – This specifies which of the n+1 hardware CoS queues the config sred command will apply to.
Restrictions	None.

Example usage

To show sred:

```
DES-3528:5#show sred
Command: show sred

Simple RED Globale Status: Disabled

Port Class Drop Green Threshold Drop Rate
          Low High Low High
-----
1 0 Disabled 60 80 1 1
1 1 Disabled 60 80 1 1
1 2 Disabled 60 80 1 1
1 3 Disabled 60 80 1 1
1 4 Disabled 60 80 1 1
1 5 Disabled 60 80 1 1
1 6 Disabled 60 80 1 1
1 7 Disabled 60 80 1 1
2 0 Disabled 60 80 1 1
2 1 Disabled 60 80 1 1
2 2 Disabled 60 80 1 1
2 3 Disabled 60 80 1 1
2 4 Disabled 60 80 1 1
2 5 Disabled 60 80 1 1
2 6 Disabled 60 80 1 1
2 7 Disabled 60 80 1 1
3 0 Disabled 60 80 1 1
```

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

show sred drop_counter

Purpose	Used to display the simple RED drop packet counter per port.
Syntax	show sred drop_counter {<portlist>}
Description	This command displays, for the egress port, the count of dropped packets
Parameters	<i>portlist</i> – A range of ports to show.
Restrictions	None.

Example usage

This example displays red and yellow packet drop counts for all ports:

```
DES-3528:5#show sred drop_counter
```

```
Command: show sred drop_counter
```

Port	Yellow	Red
1	122	3
2	0	0
3	12	14
4	5	3
5	7	5
6	243	120
7	24	32

```
DES-3528:5#
```

config dscp trust

Purpose	Used to enable/disable DSCP trust state on selected portlist.
Syntax	config dscp trust [<portlist> all] state [enable disable]
Description	This command is used to configure port DSCP trust state. When DSCP is not trusted, 1p is trusted.
Parameters	<i>portlist</i> – A range of ports to config. <i>state</i> – Enable/disable to trust DSCP. By default, DSCP trust is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

This config dscp trust:

```
DES-3528:5#config dscp trust 1-8 state enable
```

```
Command: config dscp trust 1-8 state enable
```

```
Success.
```

```
DES-3528:5#
```

show dscp trust

Purpose	Used to display DSCP trust state.
Syntax	show dscp trust {<portlist>}
Description	This command is used to display DSCP trust state.
Parameters	<i>portlist</i> – A range of ports to display.
Restrictions	None.

Example usage

To display the DSCP trust state:

```
DES-3528:5#show dscp_trust
```

```
Command: show dscp_trust
```

```
Port      DSCP-Trust
-----  -
1         Disabled
2         Disabled
3         Disabled
4         Disabled
5         Enabled
6         Enabled
7         Enabled
8         Enabled
```

```
DES-3528:5#
```

config dscp map

Purpose	Used to configure mapping of DSCP to priority and packet's initial color .																		
Syntax	config dscp map [<portlist> all] [dscp_priority <dscp_list> to <priority 0-7> dscp_dscp <dscp_list> to <dscp 0-63> dscp_color <dscp_list> to [green red yellow]]																		
Description	<p>The mapping of DSCP to COS will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.</p> <p>The mapping of dscp to color will be used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is DSCP-trusted.</p> <p>The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingress to the port. The remaining processing of the packet will be based on the new DSCP. By default, the DSCP is mapped to the same DSCP.</p>																		
Parameters	<p><i>portlist</i> – Specifies ports to be configured.</p> <p><i>dscp_priority</i> – Specifies a list of DSCP value to be mapped to a specific priority</p> <p><i>priority</i> – Specifies the result priority of mapping.</p> <p>The default mapping are:</p> <table border="1" data-bbox="375 1780 1260 1870"> <tr> <td>DSCP</td> <td>0-7</td> <td>8-15</td> <td>16-23</td> <td>24-31</td> <td>32-39</td> <td>40-47</td> <td>48-55</td> <td>56-63</td> </tr> <tr> <td>priority</td> <td>0</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>6</td> <td>7</td> </tr> </table> <p><i>dscp_dscp</i> – Specifies a list of DSCP value to be mapped to a specific dscp.</p> <p><i>dscp</i> – Specifies the result DSCP of mapping.</p> <p><i>dscp_color</i> – Specifies a list of DSCP value to be mapped to a specific color.</p> <p><i>color</i> – Specifies the result color of mapping.</p>	DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63	priority	0	1	2	3	4	5	6	7
DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63											
priority	0	1	2	3	4	5	6	7											
Restrictions	Only Administrator and Operator-level users can issue this command.																		

Example usage

This config dscp map:

```
DES-3528:5#config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

DES-3528:5#
```

show dscp map

Purpose	Used to display the DSCP map configure parameter.
Syntax	show dscp map { <portlist> } [dscp_priotity dscp_dscp dscp_color] {dscp <dscp_list>}
Description	This command is used to show DSCP trusted portlist and mapped color, priority and DSCP.
Parameters	<i>portlist</i> – Specifies a range of ports to display. <i>dscp</i> – Specifies DSCP value that will be mapped.
Restrictions	None.

Example usage

This show dscp map:

```
DES-3528:5#show dscp map dscp_color
Command: show dscp map dscp_color

DSCP to Color mapping
Port 1
  DSCP 0 - 7 is mapped to Green
  DSCP 8 - 15, 17 is mapped to Yellow
  DSCP 16, 18 - 63 is mapped to Red

DES-3528:5#
```

config 802.1p map

Purpose	Used to configure mapping of 1p to packet's initial color.
Syntax	config 802.1p map [<portlist> all] 1p_color [<priority_list>] to [green red yellow]
Description	This command is used to configure mapping of 1p to packet's initial color. The mapping of 1p to color will be used to determine the initial color of the packet, when the policing function of the packet is color aware and the packet is 1p-trusted.
Parameters	<i>portlist</i> – A range of ports to configure. <i>priority</i> – source priority of incoming packets. <i>color</i> – mapped color for packet, default value is green
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

This config 802.1p map:

```
DES-3528:5#config 802.1p map 1-8 lp_color 1 to red
Command: config 802.1p map 1-8 lp_color 1 to red
Success.

DES-3528:5#
```

show 802.1p map

Purpose	Used to display the 1p to color mapping
Syntax	show 802.1p map lp_color { <portlist>}
Description	This command is used to display the 1p to color mapping
Parameters	<i>portlist</i> – A range of ports to show.
Restrictions	None.

Example usage

This show 802.1p map:

```
DES-3528:5#show 802.1p map lp_color
Command: show 802.1p map lp_color

802.1p to Color Mapping:
-----
Port  0      1      2      3      4      5      6      7
-----
1     Green  Green  Green  Green  Green  Green  Green  Green
2     Green  Green  Green  Green  Green  Green  Green  Green
3     Green  Green  Green  Green  Green  Green  Green  Green
4     Green  Green  Green  Green  Green  Green  Green  Green
5     Green  Green  Green  Green  Green  Green  Green  Green
6     Green  Green  Green  Green  Green  Green  Green  Green
7     Green  Green  Green  Green  Green  Green  Green  Green
8     Green  Green  Green  Green  Green  Green  Green  Green
9     Green  Green  Green  Green  Green  Green  Green  Green
10    Green  Green  Green  Green  Green  Green  Green  Green
11    Green  Green  Green  Green  Green  Green  Green  Green
12    Green  Green  Green  Green  Green  Green  Green  Green
13    Green  Green  Green  Green  Green  Green  Green  Green
14    Green  Green  Green  Green  Green  Green  Green  Green
15    Green  Green  Green  Green  Green  Green  Green  Green
16    Green  Green  Green  Green  Green  Green  Green  Green
17    Green  Green  Green  Green  Green  Green  Green  Green
18    Green  Green  Green  Green  Green  Green  Green  Green

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


MLD SNOOPING COMMAND LIST

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] report_suppression [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 <vlan_name 32> vlanid <vidlist>] [add delete] <portlist>
config mld_snooping mrouter_ports_forbidden	[vlan <vlan_name 32> vlanid <vidlist>] [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> ports <portlist>] {<ipv6addr>}} {data_driven}
show mld_snooping mrouter_ports	[vlan <vlan_name 32> vlanid <vidlist> all] { [static dynamic forbidden]}
config mld_snooping rate_limit	[ports <portlist> vlanid <vidlist>] [<value 1-1000> no_limit]
show mld_snooping rate_limit	[ports <portlist> vlanid <vidlist>]
show mld_snooping forwarding	{[vlan <vlan_name 32> vlanid <vidlist>]}
create mld_snooping static_group	[vlan <vlan_name 32> vlanid <vidlist>] < ipv6addr >
config mld_snooping static_group	[vlan <vlan_name 32> vlanid <vidlist>] < ipv6addr > [add delete] <portlist>
delete mld_snooping static_group	[vlan <vlan_name 32> vlanid <vidlist>] < ipv6addr >
show mld_snooping static_group	{[vlan <vlan_name 32> vlanid <vidlist>] < ipv6addr >}
show mld_snooping statistic counter	[vlan <vlan_name 32> vlanid <vidlist> ports <portlist>]
clear mld_snooping statistic counter	
config mld_snooping data_driven_learning	[all vlan_name <vlan_name> vlanid <vidlist>] { state [enable disable] aged_out [enable disable] expiry_time <sec 1-65535>}(1)
config mld_snooping data_driven_learning max_learned_entry	<value 1-1024>

Command	Parameters
clear mld_snooping data_driven_group	[all [vlan_name <vlan_name> vlanid <vidlist>] [<ipaddr> all]]

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] report_suppression [enable disable]}(1)
Description	This command configures MLD snooping on the switch. If the MLD version is configured with a lower version, the higher version's MLD Report/Leave messages will be ignored.
Parameters	<p><i>vlan</i> – The name of the VLAN for which MLD snooping is to be configured.</p> <p><i>vlanid</i> - The ID of the VLAN for which MLD snooping is to be configured.</p> <p><i>state</i> – Allows you to enable or disable the MLD snooping function for the chosen VLAN.</p> <p><i>fast_done</i> – enable or disable MLD snooping fast done function. If it is enabled, the membership is immediately removed when the system receive the MLD done message.</p> <p><i>report_suppression</i> – When it is enabled, multiple MLD reports will be intergrated into one report before sending to the router port.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To configure the MLD snooping to the default vlan with noted_timeout 250 sec and state enable:

```
DES-3528:5# config mld_snooping vlanid 1 fast_done enable state enable
report_suppression disable
Command: config mld_snooping vlanid 1 fast_done enable state enable report_suppression
disable

Success.

DES-3528:5#
```

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 configures 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><i>vlan_name</i> – The name of the VLAN for which MLD snooping is to be configured.</p> <p><i>query_interval</i> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p><i>max_reponse_time</i> – The maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.</p> <p><i>robustness_variable</i> – 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> <p><i>group listener interval</i> – 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).</p> <p><i>other querier present interval</i> – 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).</p> <p><i>last listener query count</i> – 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> <p>By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy.</p> <p><i>last_listener_query_interval</i> – 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><i>state</i> – Allows you to enable or disable the MLD snooping function for the chosen VLAN.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To configure the MLD snooping querier query interval to 125 secs and state enable:

```
DES-3528:5#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-3528:5#
```

config mld_snooping mrouter_ports

Purpose	Used to configure ports as router ports.
Syntax	config mld_snooping mrouter_ports [vlan <vlan_name 32> vlanid <vidlist>] [add delete] <portlist>
Description	This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets sent to VLAN with the specified router port list, will be forwarded to the port list, regardless of protocols.
Parameters	<i>vlan_name</i> – The name of the VLAN for which MLD snooping is to be configured. <i>add delete</i> – Specifies to add or delete the router ports. <i>portlist</i> – Specifies a range of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To set up port range 1-10 to be static router ports:

```
DES-3528:5#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

DES-3528:5#
```

config mld_snooping mrouter_ports_forbidden

Purpose	Used to configure ports as forbidden router ports.
Syntax	config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> vlanid <vidlist>] [add delete] <portlist>
Description	This command allows you to designate a range of ports that are forbidden to connect to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Parameters	<i>vlan_name</i> – The name of the VLAN for which MLD snooping is to be configured. <i>add delete</i> – Specifies to add or delete the router ports. <i>portlist</i> – Specifies a range of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To set up port range 1-10 to static router ports:

```
DES-3528:5#config mld_snooping mrouter_ports_forbidden vlan default add 1-10
Command: config mld_snooping mrouter_ports_forbidden vlan default add 1-10

Success.

DES-3528:5#
```

enable mld_snooping

Purpose	Used to enable MLD snooping on the switch.
Syntax	enable mld_snooping
Description	This command allows you to enable MLD snooping on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To enable MLD snooping on the switch:

```
DES-3528:5#enable mld_snooping
Command: enable mld_snooping

Success.

DES-3528:5#
```

disable mld_snooping

Purpose	Used to disable MLD snooping on the switch.
Syntax	disable mld_snooping
Description	This command disables MLD snooping on the switch. Disabling MLD snooping allows all MLD and IPv6 multicast traffic to flood within all IPv6 interfaces.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To disable MLD snooping on the switch:

```
DES-3528:5#disable mld_snooping
Command: disable mld_snooping

Success.

DES-3528:5#
```

show mld_snooping

Purpose	Used to display the current status of MLD snooping on the switch.
Syntax	show mld_snooping {vlan <vlan_name 32> }
Description	This command will display the current MLD snooping configuration on the switch.
Parameters	<i>vlan_name</i> – The name of the VLAN for which you want to view the MLD snooping configuration. If no parameter specified, the system will display all current MLD snooping configurations.
Restrictions	None.

Example usage

To show MLD snooping on the switch:

```

DES-3528:5#show mld_snooping
Command: show mld_snooping

MLD Snooping Global State           : Enabled
Data Driven Learning Max Entries    : 128

VLAN Name                           : default
Query Interval                       : 125
Max Response Time                    : 10
Robustness Value                     : 2
Last Listener Query Interval         : 1
Querier State                        : Enable
Querier Role                         : Querier
Querier IP                           : FE80::221:91FF:FEAF:EA00
Querier Expiry Time                  : 0 secs
State                                : Enable
Fast Done                            : Enable
Report Suppression                   : Disable
Rate Limit                           : No Limitation
Version                              : 2
Data Driven Learning State           : Enable
Data Driven Learning Aged Out        : Disable
Data Driven Group Expiry Time        : 260

VLAN Name                           : mv1
CTRL+C  ESC  q Quit  SPACE  n Next Page  ENTER Next Entry  a All

```

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> ports <portlist>] {<ipv6addr>}} {data_driven}
Description	This command displays the current MLD snooping group configuration on the switch.
Parameters	<p><vlan_name 32> – The name of the VLAN for which you want to view the MLD snooping configuration. If no parameter is specified, the system will display all current MLD snooping group.</p> <p><vidlist> – The VIDs of the VLAN for which MLD snooping is to be configured.</p> <p><portlist> – The list of ports for which to view MLD snooping group information.</p> <p><ipv6addr> – To view the information of this specified group.</p> <p>data_driven – To view the groups learnt by data driven only.</p>
Restrictions	None.

Example usage

To show MLD snooping group on the switch:

```

DES-3528:5#show mld_snooping group
Command: show mld_snooping group

Source/Group      : 2004::2/FF1E::3
VLAN Name/VID     : default/1
Member Ports      : 1-2
UP Time           : 127
Expiry Time       : 120
Filter Mode       : INCLUDE

Source/Group      : 2004::2/FF1E::2
VLAN Name/VID     : default/1
Member Ports      : 3
UP Time           : 320
Expiry Time       : 120
Filter Mode       : EXCLUDE

Source/Group      : NULL/FF1E::5
VLAN Name/VID     : default/1
Member Ports      : 4-5
UP Time           : 130
Expiry Time       : 120
Filter Mode       : EXCLUDE

Source/Group      : NULL/FF1E::5
VLAN Name/VID     : default/1
Member Ports      :
Router Ports      : 24
UP Time           : 1335
Expiry Time       : 120
Filter Mode       : EXCLUDE

DES-3528:5#

```

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> all] {[static dynamic forbidden]}
Description	This command displays the currently configured router ports on the switch.
Parameters	<p><i>vlan_name</i> – The name of the VLAN for which you want to view the MLD snooping configuration.</p> <p><i>static</i> – Displays router ports that have been statically configured.</p> <p><i>dynamic</i> – Displays router ports that have been dynamically configured.</p> <p><i>forbidden</i> – Displays forbidden router ports that have been statically configured.</p> <p>If no parameter specified, the system will display all currently configured router ports on the switch.</p>
Restrictions	None.

Example usage

To display the router ports on the switch:

```
DES-3528:5# show mld_snooping mrouter_ports all
Command: show mld_snooping mrouter_ports all

VLAN Name           : default
Static Router Port   : T1
Dynamic Router Port  :
  Router IP          :
Forbidden Router Port :

VLAN Name           : VLAN2
Static Router Port   :
Dynamic Router Port  :
  Router IP          :
Forbidden Router Port :

Total Entries: 2
DES-3528:5#
```

config mld_snooping rate_limit

Purpose	Used to configure the MLD snooping rate limite on ports.
Syntax	config mld_snooping rate_limit [ports <portlist> vlanid <vidlist>] [<value 1-1000> no_limit]
Description	This command configures the MLD snooping rate limite on ports.
Parameters	<p><i>ports</i> – A port number or a range of ports for you to configure the MLD snooping rate limited</p> <p><i>vlanid</i> – The ID of the VLAN for which MLD snooping is to be configured.</p> <p><i>rate_limit</i> - Configures the rate of MLD control packet that the switch can process on a specific port. The rate is specified in packet per second. The packet that exceeds the limited rate will be dropped.The default setting is <i>no_limit</i>.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To configure MLD snooping rate limit:

```
DES-3528:5# config mld_snooping rate_limit port 1-4 500
Command: config mld_snooping rate_limit ports 1-4 500

Success.

DES-3528:5#
```


show mld_snooping rate_limit

Purpose	Used to display the MLD snooping rate limite on ports.
Syntax	show mld_snooping rate_limit [ports <portlist> vlanid <vidlist>]
Description	This command displays the MLD snooping rate limite on ports.
Parameters	<i>ports</i> – A port number or a range of ports for you to view the MLD snooping rate limited. <i>vlanid</i> – The id of the VLAN for which MLD snooping is to be displayed.
Restrictions	None.

Example usage

To display the MLD snooping rate limit:

```
DES-3528:5# show mld_snooping rate_limit ports 1-4
```

```
Command: show mld_snooping rate_limit ports 1-4
```

Port	Rate Limitation
-----	-----
1	500
2	500
3	500
4	500

```
Total Entries: 4
```

```
DES-3528:5#
```

show mld_snooping forwarding

Purpose	Used to display the current MLD snooping forwarding table.
Syntax	show mld_snooping forwarding {[vlan <vlan_name 32> vlanid <vidlist>]}
Description	This command displays the current MLD snooping forwarding table. It provides an easy way for user to check the list of ports that a specific source of a multicast group will be forwarded to.
Parameters	<i>vlan</i> – The name of the VLAN for which you want to view MLD snooping forwarding table information. If no parameter is specified, the system will display all current MLD snooping forwarding table entries. <i>vlanid</i> – The ID of the VLAN for which you want to view MLD snooping forwarding table information. If no parameter is specified, the system will display all current MLD snooping forwarding table.
Restrictions	None.

Example usage

To display the MLD snooping rate limit:

```
DES-3528:5# show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name      : default
Source IP      : 2004::1
Multicast Group: FF1E::1
Port Member    : 2,7

VLAN Name      : default
Source IP      : 2004::2
Multicast Group: FF1E::1
Port Member    : 2,5

VLAN Name      : default
Source IP      : 2004::2
Multicast Group: FF1E::2
Port Member    : 2,8

Total Entries : 3

DES-3528:5#
```

create mld_snooping static_group

Purpose	Used to configure a MLD Snooping multicast static group.
Syntax	create mld_snooping static_group [vlan <vlan_name 32> vlanid <vidlist>] < ipv6addr >
Description	<p>This command is used to create a mld snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group.</p> <p>The static group will only take effect when MLD snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the MLD protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.</p> <p>The device is also responsible to route the packet destined for this specific group to static member ports.</p> <p>The static member port will only affect V2 MLD operation.</p> <p>The Reserved IP multicast address 224.0.0.X must be excluded from the configured group.</p> <p>The VLAN must be created first before a static group can be created.</p>
Parameters	<p><i>vlan</i> – The name of the VLAN that has been configured.</p> <p><i>vlanid</i> – The ID of the VLAN that has been configured.</p> <p><i>ipaddr</i> – Specifies the multicast group IP address. (for Layer 3 switch)</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To create a mld snooping static group for VLAN 1, group 239.1.1.1:

```
DES-3528:5#create mld_snooping static_group vlan default FF1E::1
Command: create mld_snooping static_group vlan default FF1E::1

Success.

DES-3528:5#
```

config mld_snooping static_group

Purpose	Used to configure a MLD Snooping multicast group static member port.
Syntax	config mld_snooping static_group [vlan <vlan_name 32> vlanid <vidlist>] < ipv6addr > [add delete] <portlist>
Description	When a port is configured as a static member port, the MLD protocol will not operate on this port. Therefore, supposed that a port is a dynamic member port learned by MLD. If this port is configured as a static member later, then the MLD protocol will stop operating on this port. The MLD protocol will resume once this port is removed from static member ports. The static member port will only affect MLD v1 operation.
Parameters	<i>vlan</i> – The name of the VLAN that has been configured. <i>vlanid</i> – The ID of the VLAN that has been configured. <i>ipaddr</i> – Specifies the multicast group IP address. (for Layer 3 switch) <i>add delete</i> – Specifies to add or delete the member ports. <i>portlist</i> – Specifies a port number or a range of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To unset port range 9-10 from MLD Snooping static member ports for group 239.1.1.1 on default VLAN:

```
DES-3528:5#config mld_snooping static_group vlan default FF1E::1 add 2:9-2:10
Command: config mld_snooping static_group vlan default FF1E::1 add 2:9-2:10

Success.

DES-3528:5#
```

delete mld_snooping static_group

Purpose	Used to delete a MLD Snooping multicast static group.
Syntax	delete mld_snooping static_group [vlan <vlan_name 32> vlanid <vidlist>] < ipv6addr >
Description	This command is used to delete a MLD Snooping multicast static group, and will not affect the MLD snooping dynamic member ports for a group.
Parameters	<i>vlan</i> – The name of the VLAN on which the router port resides. <i>vlanid</i> – The ID of the VLAN on which the router port resides. <i>ipaddr</i> – Specifies the multicast group IP address. (for Layer 3 switch)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To unset port range 9-10 from MLD Snooping static member ports for group 239.1.1.1 on default VLAN:

```
DES-3528:5#delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

DES-3528:5#
```

show mld_snooping static_group

Purpose	Used to display a MLD Snooping multicast group static member port.
Syntax	show mld_snooping static_group {[vlan <vlan_name 32> vlanid <vidlist>] < ipv6addr >}
Description	This command is used to display a MLD Snooping multicast group static member port.
Parameters	<i>vlan</i> – The name of the VLAN on which the router port resides. <i>vlanid</i> – The ID of the VLAN on which the router port resides. <i>ipaddr</i> – Specifies the multicast group IP address. (for Layer 3 switch)
Restrictions	None.

Example usage

To display all the MLD snooping static groups:

```
DES-3528:5# show mld_snooping static_group
Command: show mld_snooping static_group

VLAN ID/Name          IP Address          Static Member Ports
-----
1 / Default          FF1E ::1           2:9-2:10

Total Entries : 1

DES-3528:5#
```

show mld_snooping statistic counter

Purpose	Used to display a MLD Snooping statistics counter.
Syntax	show mld_snooping statistic counter [vlan <vlan_name 32> vlanid <vidlist> ports <portlist>]
Description	This command displays the statistics counter for MLD protocol packets that are received by the switch since MLD Snooping is enabled.
Parameters	<i>vlan</i> – The name of the VLAN on which the router port resides. <i>vlanid</i> – The ID of the VLAN on which the router port resides. <i>ports</i> – Specifies a port number or a range of ports to be displayed.
Restrictions	None.

Example usage

To display MLD Snooping statistic counter:

```
DES-3528:5# show mld_snooping statistic counter vlanid 1
Command: show mld_snooping statistic counter vlanid 1

VLAN Name   : Default
-----
Total Groups           : 10
Receive Statistics
  Query
    MLD v1 Query       : 1
    MLD v2 Query       : 1
    Total               : 2
    Dropped By Rate Limitation : 1
    Dropped By Multicast VLAN : 1

  Report & Done
    MLD v1 Report      : 0
    MLD v2 Report      : 10
    MLD v1 Done        : 1
    Total              : 21
    Dropped By Rate Limitation : 0
    Dropped By Max Group Limitation : 90
    Dropped By Group Filter : 0
    Dropped By Multicast VLAN : 1

Transmit Statistics
  Query
    MLD v1 Query       : 1
    MLD v2 Query       : 1
    Total               : 2
  Report & Done
    MLD v1 Report      : 0
    MLD v2 Report      : 10
    MLD v1 Done        : 1
    Total              : 11

Total Entries : 1

DES-3528:5#
```

clear mld_snooping statistic counter

Purpose	Used to clear the current MLD snooping statistic on the Switch.
Syntax	clear mld_snooping statistic counter
Description	All MLD snooping statistic counters will be cleared.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear IGMP snooping statistic counter:


```
DES-3528:5#clear mld_snooping statistic counter
```

```
Command: clear mld_snooping statistic counter
```

```
Success.
```

```
DES-3528:5#
```

config mld_snooping data_driven_learning

Purpose	Used to configure the data driven learning of a MLD snooping group.
Syntax	config mld_snooping data_driven_learning [all vlan_name <vlan_name> vlanid <vidlist>] { state [enable disable] aged_out [enable disable] expiry_time <sec 1-65535>}(1)
Description	<p>This command is used to configure the data driven learning of a MLD snooping group.</p> <p>When data-driven learning is enabled for the VLAN, the switch receives the IP multicast traffic on this VLAN, and a MLD snooping group will be created. The learning of an entry is not activated by MLD membership registration, but by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care that the ageing out of the entry. For a data-driven entry, the entry can be specified so that it doesnt ageout or ageout by the aged timer.</p> <p>When data driven learning is enabled, and data driven table is not full, the multicast filtering mode for all ports are ignored. The multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.</p>
	 <p>NOTE: If a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. That is, the ageing out mechanism will follow the ordinary MLD snooping entry.</p>
Parameters	<p><i>vlan_name</i> <vlan_name> – The name of the VLAN for which MLD snooping data driven learning is to be configured.</p> <p><i>vlanid</i> <vidlist> – The VID of the VLAN for which MLD snooping data driven learning is to be configured.</p> <p><i>state</i> [enable disable] – Allows users to enable or disable MLD snooping data driven learning for the specified VLAN.</p> <p><i>aged_out</i> [enable disable] – Allows users to enable or disable the aged_out time of the MLD Snooping data driven learning for the specified VLAN.</p> <p><i>expiry_time</i> <second> – Allows users to set the time that an MLD Snooping data driven learning group will expire for the specified VLAN.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable data driven learning on VLAN default:

```
DES-3528:5# config mld_snooping data_driven_learning vlan_name default state enable aged_out enable expiry_time 270
```

```
Command: config mld_snooping data_driven_learning vlan_name default state enable aged_out enable expiry_time 270
```

```
Success.
```

```
DES-3528:5#
```

config mld_snooping data_driven_learning max_learned_entry

Purpose	Used to configure the max number of groups that can be learned by data driven.
Syntax	config mld_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 the new data-driven groups. Traffic for the new groups will be dropped.
Parameters	<value 1-1024 > – The max number of groups that can be learned by data driven.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the max number of groups that can be learned by data driven:

```
DES-3528:5#config mld_snooping data_driven_learning max_learned_entry 100
Command: config mld_snooping data_driven_learning max_learned_entry 100

Success.

DES-3528:5#
```

clear mld_snooping data_driven_group

Purpose	Used to delete the MLD snooping group learned by data driven.
Syntax	clear mld_snooping data_driven_group [all [vlan_name <vlan_name> vlanid <vidlist>] [<ipv6addr > all]]
Description	This command is used to delete the MLD snooping group learned by data driven.
Parameters	<i>all</i> – Delete all groups learnt by data driven. <i>vlan_name <vlan_name 32></i> – The name of the VLAN for which MLD snooping data driven learning group is to be deleted. <i>vlanid <vidlist></i> – The VID of the VLAN for which MLD snooping data driven learning group is to be deleted. <i><ipv6addr></i> – The group address for which MLD snooping data driven learning group is to be deleted on the specified VLAN. <i><all></i> – All groups learnt by data driven on the specified VLAN will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete all groups learnt by data driven on VLAN default:

```
DES-3528:5#clear mld_snooping data_driven_group vlan_name default all
Command: clear mld_snooping data_driven_group vlan_name default all

Success.

DES-3528:5#
```

MAC-BASED ACCESS CONTROL COMMANDS LIST

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 guest_vlan ports	<portlist>
config mac_based_access_control ports	[<portlist> all] {state [enable disable] mode [port_based host_based] aging_time [infinite <min 1-1440>] block_time[infinite <sec 1-300>] max_users [<value 1 - 1000> no_limit]}(1)
create mac_based_access_control	[guest_vlan <vlan_name 32> guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control	[guest_vlan <vlan_name 32> guest_vlanid <vlanid 1-4094>]
clear mac_based_access_control auth_state	[ports [all portlist] mac_addr <macaddr>]
create mac_based_access_control_local mac	<macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094>]
config mac_based_access_control_local mac	<macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094> clear_vlan]
delete mac_based_access_control_local	[mac <macaddr> vlan <vlan_name 32> vlanid <vlanid 1-4094>]
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 auth_failover	[enable disable]
config mac_based_access_control authorization network	{radius [enable disable] local [enable disable]}(1)
config mac_based_access_control max_users	[<value 1 - 1000> no_limit]

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 will enable the MAC-based AC function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To enable MAC-based AC function:

```
DES-3528:5#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DES-3528:5#
```

disable mac_based_access_control

Purpose	Used to disable MAC-based AC.
Syntax	disable mac_based_access_control
Description	This command will disable the MAC-based AC function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To disable MAC-based AC function:

```
DES-3528:5#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DES-3528:5#
```

config mac_based_access_control password

Purpose	Used to configure the password of the MAC-based AC.
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	<passwd 16> – In RADIUS mode, the switch communicate with RADIUS server use the password. The maximum length of the key is 16.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To configure MAC-based AC password:

```
DES-3528:5# config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

DES-3528:5#
```

config mac_based_access_control method

Purpose	Use to configure the MAC-based AC authenticating method.
Syntax	config mac_based_access_control method [local radius]
Description	This command is used to specify to authenticate via local database or via RADIUS server.
Parameters	<i>local</i> – Specify to authenticate via local database. <i>radius</i> – Specify to authenticate via RADIUS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure mac based access control authenticating method:

```
DES-3528:5#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DES-3528:5#
```

config mac_based_access_control guest_vlan ports

Purpose	Use to configure the MAC-based AC guest VLAN membership.
Syntax	Config mac_based_access_control guest_vlan ports <portlist>
Description	This command is used to put the specified port in guest VLAN mode. For those ports that are not contained in the port list, they are in non-guest VLAN mode. For detailed information about operation of guest VLAN mode, refer to the description for config mac_based_access_control port command.
Parameters	<portlist> – When the guest VLAN is configured for a port successfully, the port will make the VLAN assignment based on the assigned VLAN and remove it from the guestvlan. If the user authentication fails, the user will stay in the guestvlan mode.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To create MAC-based AC guest VLAN:

```
DES-3528:5#create mac_based_access_control_guest_vlan default
Command: create mac_based_access_control_guest_vlan default

Success.

DES-3528:5#
```

config mac_based_access_control_ports

Purpose	Used to configure the parameter of the MAC-based AC.
Syntax	config mac_based_access_control_ports [<portlist> all] {state [enable disable] mode [port_based host_based] aging_time [infinite <min 1-1440>] block_time[infinite <sec 1-300>] max_users [<value 1 - 1000> no_limit]}(1)
Description	<p>This command allows you to configure MAC-based AC setting.</p> <p>When the MAC-based AC is enabled for a port, and the guest VLAN function for this port is disabled, the user attached to this port will not forward any packets unless the user passes authentication. The user that does not pass authentication will not be serviced by the switch. If the user passes authentication, the user will be able to forward traffic operated under the assigned VLAN configuration.</p> <p>When the MAC-based 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, 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 is assigned from the RADIUS Server or the VLAN assigned by RADIUS server is invalid (e.g. the assigned VLAN is not existent), this port/MAC will be removed from the member port of the guest VLAN and become a member port of the original VLAN</p>
Parameters	<p><i>ports</i> – A range of ports enable or disable mac_based_access_control function.</p> <p><i>state</i> – Specify whether MAC-based AC function is enabled or disabled.</p> <p><i>mode</i> – Either port_based or host_based.</p> <p>Port_based: means that all users connected to a port share the first authentication result.</p> <p>Host_based: means that each user can have its own authentication result. If the Switch doesn't support MAC-Based VLAN, then the switch will not allow the option host_based for ports that are in guest vlan mode.</p> <p><i>method</i> – Specify which authenticated method.</p> <p><i>aging_time</i> – A time period during which an authenticated host will be kept in authenticated state. When the aging time is time-out, the host will be moved back to unauthenticated state.</p> <p><i>block_time</i> – If a host fails to pass the authentication, the next authentication will not started within block_time unless the user clear the entry state manually.</p> <p><i>max_user</i> – max number of authenticated clients on per port.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config port state:

```
DES-3528:5#config mac_based_access_control_ports 1-8 state enable
Command: config mac_based_access_control_ports 1-8 state enable

Success.

DES-3528:5#
```

To config port mode:

```
DES-3528:5#config mac_based_access_control_ports 1-8 mode port_based
Command: config mac_based_access_control_ports 1-8 mode port_based
Success.

DES-3528:5#
```

create mac_based_access_control

Purpose	Used to create the guest_vlan
Syntax	create mac_based_access_control [guest_vlan <vlan_name 32> guest_vlanid <vlanid 1-4094>]
Description	This command is used to create the guest VLAN.
Parameters	<i>guest_vlan</i> – If the MAC address has failed the authentication, the port will be assigned to this vlan. <i>guest_vlanid</i> – If the MAC address has failed the authentication, the port will be assigned to this vlan.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create mac based access control guest vlan:

```
DES-3528:5#create mac_based_access_control guest_vlan default
Command: create mac_based_access_control guest_vlan default
Success.

DES-3528:5#
```

delete mac_based_access_control

Purpose	Used to delete the 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	<i>guest_vlan</i> – Specifies the name of the guest_vlan. <i>guest_vlanid</i> – Specifies the vlan_id of the guest_vlan.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a guest vlan:

```
DES-3528:5#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

DES-3528:5#
```

clear mac_based_access_control auth_state

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_state [ports [all portlist] mac_addr <macaddr>]
Description	This command is used to clear the authentication state of a user (or port) . The port (or the user) will return to un - authenticated state. All the timer associated with the port (or the user) will be reset.
Parameters	<i>ports</i> – To specify the port range to delete MAC on them <macaddr> – To delete a specified host with this MAC
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear MAC auth_state on MAC enable ports:

```
DES-3528:5#clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DES-3528:5#
```

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 a database entry.
Parameters	<i>mac</i> – The MAC address that access accept by local mode <i>vlan</i> – If the MAC address is authorized, the port will be assigned to this vlan. <i>vlanid</i> – If the MAC address is authorized, the port will be assigned to this vlan.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a local database entry:

```
DES-3528:5#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-3528:5#
```

config mac_based_access_control_local mac

Purpose	Used to config the local database entry.
Syntax	config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094>]
Description	This command is used to modify a database entry.
Parameters	<i>mac</i> – The MAC address that access accept by local mode <i>vlan</i> – If the MAC address is authorized, the port will be assigned to this vlan. <i>vlanid</i> – If the MAC address is authorized, the port will be assigned to this vlan.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a local database entry:

```
DES-3528:5#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-3528:5#
```

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 a database entry.
Parameters	<i>mac</i> – Deletes the database entry by this MAC address. <i>vlan</i> – Deletes the database entry by this VLAN name. <i>vlanid</i> – Deletes the database entry by this VLAN id.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the local database entry by mac address:

```
DES-3528:5#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-3528:5#
```

To delete the local database entry by vlan name:

```
DES-3528:5#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

DES-3528:5#
```

show mac_based_access_control

Purpose	Used to display mac_based_access_control setting.
Syntax	show mac_based_access_control {ports {<portlist>}}
Description	This command is used to display mac_based_access_control settings.
Parameters	<i>ports</i> – Display mac_based_access_control port state
Restrictions	None.

Example usage:

To display mac based access control settings:

```
DES-3528:5#show mac_based_access_control ports 1-7
Command: show mac_based_access_control ports 1:1-1:7
```

Port	State	Aging Time (mins)	Block Time (secs)	Auth Mode	Max User
1:1	Disabled	1440	300	Host_based	128
1:2	Disabled	1440	300	Host_based	128
1:3	Disabled	1440	300	Host_based	128
1:4	Disabled	1440	300	Host_based	128
1:5	Enabled	1440	300	Host_based	128
1:6	Enabled	1440	300	Host_based	128
1:7	Enabled	1440	300	Host_based	128

```
DES-3528:5#
```

show mac_based_access_control_local

Purpose	Used to display mac_based_access_control local database.
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 database.
Parameters	<i>mac</i> – Display mac_based_access_control local database by this MAC address <i>vlan</i> – Display mac_based_access_control local database by this VLAN name. <i>vlanid</i> – Display mac_based_access_control local database by this VLAN id.
Restrictions	None.

Example usage:

To display mac based access control local:

```
DES-3528:5#show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address          VID
-----
00-00-00-00-00-01   1
00-00-00-00-00-02  123
00-00-00-00-00-03  123
00-00-00-00-00-04   1

Total Entries:4

DES-3528:5#
```

To display mac based access control local by mac address:

```
DES-3528:5#show mac_based_access_control_local mac 00-00-00-00-00-01
Command: show mac_based_access_control_local mac 00-00-00-00-00-01

MAC Address          VID
-----
00-00-00-00-00-01   1

Total Entries:1

DES-3528:5#
```

To display mac based access control local by vlan:

```
DES-3528:5#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address          VID
-----
00-00-00-00-00-01   1
00-00-00-00-00-04   1

Total Entries:2

DES-3528:5#
```

show mac_based_access_control_auth_state

Purpose	Used to display mac_based_access_control authenticated state setting.
Syntax	show mac_based_access_control_auth_state ports <portlist>
Description	This command is used to display mac_based_access_control settings.
Parameters	<i>ports</i> – Display mac_based_access_control port state
Restrictions	None.

Example usage:

To display mac based access control auth state:


```
DES-3528:5#show mac_based_access_control auth_state ports 1-7
Command: show mac_based_access_control auth_state ports 1:1-1:7
```

Port	MAC Address	State	VID	Priority	Aging Time/ Block Time

```
Total Authenticating Hosts : 0
Total Authenticated Hosts   : 0
Total Blocked Hosts         : 0
```

```
DES-3528:5#
```

config mac_based_access_control auth_failover

Purpose	Used to configure the MAC-based AC authentication failover function.
Syntax	config mac_based_access_control auth_failover [enable disable]
Description	When the authentication failover is disabled and if the Radius servers are unreachable, the authentication will fail. When the authentication failover is enabled, and if the Radius servers authentication is unreachable, the local database will be used to do the authentication. The state is disabled, by default.
Parameters	<i>enable</i> – Enables the authentication database fail over. <i>disable</i> – Disables the authentication database fail over.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the mac_based_access_control auth_failover:

```
DES-3528:5#config mac_based_access_control auth_failover enable
Command: config mac_based_access_control auth_failover enable
```

```
Success.
```

```
DES-3528:5#
```

config mac_based_access_control authorization network

Purpose	Used to enable or disable the accepting of authorized configuration.
Syntax	config mac_based_access_control authorization network {radius [enable disable] local [enable disable]}(1)
Description	This command is used to enable or disable the accepting of authorized configuration. When the authorization is enabled for MAC-AC's radius, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. When the authorization is enabled for MAC-AC's local, the authorized data assigned by the local database will be accepted.
Parameters	<i>radius</i> – If specified to enable, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. The default state is enabled. <i>local</i> – If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC-based AC authorized network:

```
DES-3528:5#config mac_based_access_control authorization network local disable
Command: config mac_based_access_control authorization network local disable

Success.

DES-3528:5#
```

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 [<value 1-1000> no_limit]
Description	The setting is a global limitation on the maximum number of users that can be learned via MAC-based AC. In addition to the global limitation, the per port maximum number of users is also limited. It is specified by config config mac_based_access_control ports max_users.
Parameters	<i>value 1-4000</i> – Specifies to set the max number of authorized clients on the whole device. <i>no_limit</i> – Specifies to not limit the system's maximum number of users. The default is 128.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC-based AC maximum number of users:

```
DES-3528:5#config mac_based_access_control max_users 126
Command: config mac_based_access_control max_users 126

Success.

DES-3528:5#
```

MULTIPLE AUTHENTICATION COMMANDS

The Multiple Authentication commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create authentication guest_vlan	[vlan <vlan_name 32> vlanid <vlanid 1-4094>]
delete authentication guest_vlan	[vlan <vlan_name 32> vlanid <vlanid 1-4094>]
config authentication guest_vlan	[vlan <vlan_name 32> vlanid <vlanid 1-4094>] [add delete] ports [<portlist> all]
config authentication ports	[<portlist> all] {auth_mode [port_based host_based] multi_authen_methods [none any dot1x_impb impb_jwac]}(1)
show authentication guest_vlan	
show authentication ports	{<portlist>}
enable authorization network	
disable authorization network	
show authorization	

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

create authentication guest_vlan

Purpose	Used to assign a static VLAN to be guest VLAN.
Syntax	create authentication guest_vlan [vlan <vlan_name 32> vlanid <vlanid 1-4094>]
Description	This command will assign a static vlan to be a guest vlan. The specific VLAN which is assigned to a guest vlan must exist first. The specific VLAN which has been assigned to a guest VLAN can't be deleted. For further description of this command please see description for config authentication guest_vlan ports .
Parameters	<i>vlan_name 32</i> – Specifies the guest vlan by VLAN name. <i>vlanid</i> – Specifies the guest vlan by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an authentication guest VLAN:

```
DES-3528:5#create authentication guest_vlan vlan Accounting
Command: create authentication guest_vlan vlan Accounting

Success.

DES-3528:5#
```

delete authentication guest_vlan

Purpose	Used to delete a configured authentication Guest VLAN.
Syntax	delete authentication guest_vlan [vlan <vlan_name 32> vlanid <vlanid 1-4094>]
Description	This command will delete the guest VLAN settings, but will not delete the static VLAN. All ports which have an enabled guest VLAN will move to the original VLAN after the guest vlan has been deleted.
Parameters	<i>vlan_name 32</i> – Specifies the guest vlan by VLAN name. <i>vlanid</i> – Specifies the guest vlan by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an authentication guest VLAN:

```
DES-3528:5#5#delete authentication guest_vlan vlan Accounting
Command: delete authentication guest_vlan vlan Accounting

Success.

DES-3528:5#
```

config authentication guest_vlan

Purpose	Used to configure the security port(s) as a specific guest VLAN member.
Syntax	config authentication guest_vlan [vlan <vlan_name 32> vlanid <vlanid 1-4094>] [add delete] ports [<portlist> all]
Description	This command is used to assign or remove ports to/ from guest VLAN. If Multiple-authentication mode is none: This port is doing the single authentication. The port will operate based on the guest VLAN configured by the single authentication module's command. If the single authentication module's guest VLAN command (for example, JWAC has no guest VLAN command) is not available, the port will not be in guest VLAN mode. If Multiple-authentication mode is not none: The port is doing the multiple authentication. The port will be operated based on the guest VLAN configured by the common authentication command.
Parameters	<i>vlan_name</i> – Assign a name of a guest VLAN. The VLAN must be an existing static VLAN. <i>vlanid</i> – Assign a VLAN ID of a guest VLAN. The VLAN must be an existing static VLAN. <i>add</i> – Specifies to add a port list to the guest VLAN. <i>delete</i> – Specifies to delete a port list from the guest VLAN. <i>portlist</i> – Specifies the configured port(s).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure authentication guest VLAN ports:

```
DES-3528:5#5#config authentication guest_vlan vlan RG add ports all
Command: config authentication guest_vlan vlan RG add ports all

Success.

DES-3528:5#
```

config authentication ports

Purpose	Used to configure security ports.
Syntax	config authentication ports [<portlist> all] {auth_mode [port_based host_based] multi_authen_methods [none any dot1x_impb impb_jwac]}(1)
Description	<p>This command is used to configure the authorization mode and authentication method on ports.</p> <p>If Multiple-authentication mode is none: This port is doing the single authentication. The port will be operated based on the auth mode configured by the single authentication module's command.</p> <p>If Multiple-authentication mode is not none: The port is doing the multiple authentication. The port will be operated based on the auth mode configured by the multiple authentication command.</p> <p>The enable/disable settings of individual authentication will always take effect. Suppose that the Multiple-authentication method of a port is set to any but MAC is disabled, JWAC and 802.1X are enabled, then the user must pass either JWAC or 802.1X method. Suppose that the Multiple-authentication method of a port is set to impb_jwac but JWAC is disabled and IMPB is enabled, then the authentication result will be the result of IMPB authentication.</p>
Parameters	<p><i>portlist</i> – Specifies the ports to be configured.</p> <p><i>auth_mode</i> – Choose between Port-based or Host-based.</p> <p>Port-based: If one of the attached hosts passes the authentication process, all hosts on the same port will be granted access to the network. If the user fails the authorization process, this port will keep trying the next authentication.</p> <p>Host-based: Every user can be authenticated individually.</p> <p><i>multi_authen_methods</i> – Specifies the method for multiple authentication.</p> <p><i>none</i> – Specifies that multiple authentication is not enabled.</p> <p><i>any</i> – If any one of the authentication methods (802.1x, MAC and JWAC) are passed, then authentication will be passed.</p> <p><i>dot1x_impb</i> – Dot1x will be verified first, and then IMPB will be verified. Both authentication methods need to be passed.</p> <p><i>impb_jwac</i> – IMPB will be verified first, and then JWAC will be verified. Both authentication methods need to be passed.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authentication mode of all ports to host based:

```
DES-3528:5#config authentication ports all auth_mode host_based
Command: config authentication ports all auth_mode host_based
```

Success.

```
DES-3528:5#
```

To configure the multi-authentication method of all ports to any:

```
DES-3528:5#5#config authentication ports all multi_authen_methods any
Command: config authentication ports all multi_authen_methods any
```

Success.

```
DES-3528:5#
```

show authentication guest_vlan

Purpose	Used to display the guest VLAN settings.
Syntax	show authentication guest_vlan
Description	This command allows you to show the information of the guest vlan.
Parameters	None.
Restrictions	None.

Example usage:

To display the guest VLAN settings on the Switch:

```
DES-3528:5#show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID          :1
Guest VLAN Member Ports:4

Total Entries: 1

DES-3528:5#
```

show authentication ports

Purpose	Used to display authentication settings on port(s).
Syntax	show authentication ports {<portlist>}
Description	This command is used to display the authentication method and authorization mode on ports.
Parameters	<i>portlist</i> – Displays multiple authentication on specific port(s).
Restrictions	None.

Example usage:

To display authentication settings for all ports:

```
DES-3528:5#show authentication ports
Command: show authentication ports

Port      Methods          Authorized Mode
-----
1:1       Any              Host_based
1:2       Any              Host_based
1:3       Any              Host_based
1:4       Any              Host_based
1:5       Any              Host_based
1:6       Any              Host_based
1:7       Any              Host_based
1:8       Any              Host_based
1:9       Any              Host_based
1:10      Any              Host_based
1:11      Any              Host_based
1:12      Any              Host_based
1:13      Any              Host_based
1:14      Any              Host_based
1:15      Any              Host_based
1:16      Any              Host_based
1:17      Any              Host_based
1:18      Any              Host_based
1:19      Any              Host_based
1:20      Any              Host_based
```

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

enable authorization network

Purpose	Used to enable authorization on the Switch.
Syntax	enable authorization network
Description	This command is used to enable the authorization network. When the authorization for network is enabled, whether the authorized data assigned by the RADIUS server will be accepted will depend on the individual module's setting. Authorization for the network is enabled by default.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the authorization network:

```
DES-3528:5#enable authorization network
Command: enable authorization network

Success.

DES-3528:5#
```

disable authorization network

Purpose	Used to disable authorization on the Switch.
Syntax	disable authorization network
Description	This command is used to disable the authorization network. When the authorization for network is disabled, the authorization data assigned by the RADIUS server will not be accepted and take effect. Authorization for the network is enabled by default.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the authorization network:

```
DES-3528:5#disable authorization network
Command: disable authorization network

Success.

DES-3528:5#
```

show authorization

Purpose	Used to show authorization status.
Syntax	show authorization
Description	This command displays the current authorization status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show authorization:

```
DES-3528:5#show authorization
Command: show authorization

Authorization for Network: Enabled

DES-3528:5#
```


WEB-BASED ACCESS CONTROL COMMANDS

The Web-based Access Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable wac	
disable wac	
config wac auth_failover	[enable disable]
config wac authorization network	{radius [enable disable] local[enable disable]}(1)
config wac clear_default_redirpath	
config wac default_redirpath	<string 128>
config wac method	[local radius]
config wac ports	[<portlist> all] {state [enable disable] aging_time [infinite <min 1-1440>] idle_time [infinite <min 1-1440>] block_time [<sec 0-300>]}(1)
config wac switch_http_port	<tcp_port_number 1-65535> {[http https]}
config wac user	<username 15> [vlan <vlan_name 32> vlanid <vlanid 1-4094>] clear_vlan]
config wac virtual_ip	<ipaddr>
show wac auth_state ports	
create wac user	<username 15>{[vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
delete wac user	[user <username 15> all_user]
show wac	{ports <portlist> all}
show wac user	
clear wac auth_state ports	[<portlist> all] {authenticated authenticating blocked }

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

enable wac

Purpose	Used to enable the Web-based access control function.
Syntax	enable wac
Description	This command will enable the WAC function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the WAC function:

```
DES-3528:5#enable wac
Command: enable wac

Success.

DES-3528:5#
```

disable wac

Purpose	Used to disable the Web-based access control function.
Syntax	disable wac
Description	This command will disable the WAC function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the WAC function:

```
DES-3528:5#disable wac
Command: disable wac

Success.

DES-3528:5#
```

config wac auth_failover

Purpose	Used to configure WAC authorization failover.
Syntax	config wac 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 servers authentication are unreachable, the local database will be used to do the authentication. The default state is disabled.
Parameters	<i>enable</i> – Enables the protocol authentication fail over. <i>disable</i> – Disables the protocol authentication fail over.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WAC authentication failover:

```
DES-3528:5#config wac auth_failover enable
Command: config wac auth_failover enable

Success.

DES-3528:5#
```

config wac authorization network

Purpose	Used to enable the acceptance of an authorized configuration.
Syntax	config wac authorization network {radius [enable disable] local [enable disable]}(1)
Description	This command is used to configure the acceptance of an authorized configuration. When the authorization is enabled for WAC's radius, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is also enabled. When the authorization is enabled for WAC's local, the authorized data assigned by the local database will be accepted.
Parameters	<i>radius</i> – If enabled, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. The default state is enabled. <i>local</i> – If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure WAC authorization from the local database:

```
DES-3528:5#config wac authorization network local disable
Command: config wac authorization network local disable

Success.

DES-3528:5#
```

config wac clear_default_redirpath

Purpose	Used to clear the WAC default redirect path.
Syntax	config wac clear_default_redirpath
Description	When the string is cleared, the client will not be redirected to another URL after successful authentication.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WAC clear default redirect path:

```
DES-3528:5#config wac clear_default_redirpath
Command: config wac clear_default_redirpath

Success.

DES-3528:5#
```

config wac default_redirpath

Purpose	Used to config wac default redirect path.
Syntax	config wac default_redirpath <string 128>
Description	If the default redirect path is configured, the user will be redirected to the default redirect path after successful authentication. When the string is cleared, the client will not be redirected to another URL after successful authentication.
Parameters	<i><string 128></i> – The URL that the client will be redirected to after successful authentication. The redirected path is cleared by default.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WAC default redirect path:

```
DES-3528:5#config wac default_redirpath http://2.3.2.3
Command: config wac default_redirpath http://2.3.2.3

Success.

DES-3528:5#
```

config wac method

Purpose	Used to configure the global parameter of the web authentication.
Syntax	config wac method [local radius]
Description	This command configures the global parameter for Web authentication.
Parameters	<i>method</i> – Specifies the authenticated method. <i>local</i> – The authentication will be done via the local database. <i>radius</i> – The authentication will be done via the RADIUS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authentication method:

```
DES-3528:5#config wac method radius
Command: config wac method radius

Success.

DES-3528:5#
```

config wac ports

Purpose	Used to configure WAC port level settings on the Switch.
Syntax	config wac ports [<portlist> all] {state [enable disable] aging_time [infinite <min 1-1440>] idle_time [infinite <min 1-1440>] block_time [<sec 0-300>]}(1)
Description	This command is used to configure WAC port level settings on the Switch.
Parameters	<p><i>state</i> – Specifies to enable/disable WAC state.</p> <p><i>aging_time</i> – A time period during which an authenticated host will be kept in authenticated state. “infinite” indicates the authenticated host on the port will not ageout. The default value is 24 hours.</p> <p><i>idle_time</i> – A time period after which an authenticated host will be moved to an un-authenticated state if there is no traffic during that period. “infinite” indicates the host will not be removed from the authenticated state due to the idle of traffic. The default value is infinite.</p> <p><i>block_time</i> – If a host fails to pass the authentication, it will be blocked for this period of time before it can be re-authenticated. The default value is 60 seconds.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port WAC state:

```
DES-3528:5#config wac ports 1-8 state enable
Command: config wac ports 1:1-1:8 state enable

Success.

DES-3528:5#
```

config wac switch_http_port

Purpose	Used to configure the TCP port that the WAC Switch listens to.
Syntax	config wac switch_http_port <tcp_port_number 1-65535> {[http https]}
Description	<p>This command is used to identify the HTTP or HTTPs packets that will be trapped to the CPU for authentication processing, or to access the login page.</p> <p>If not specified, the default port number for HTTP is 80, and the default port number for HTTPS is 443.</p> <p>If no protocol is specified, the protocol is HTTP.</p> <p>The HTTP cannot run at TCP port 443, and the HTTPS cannot run at TCP port 80.</p>
Parameters	<p><i><tcp_port_number 1-65535></i> – A TCP port which the WAC Switch listens to and uses to finish the authenticating process.</p> <p><i>http</i> – To specify that WAC runs HTTP protocol on this TCP port.</p> <p><i>https</i> – To specify that WAC runs HTTPS protocol on this TCP port.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WAC switch http port:

```
DES-3528:5# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DES-3528:5#
```

config wac user

Purpose	Used to configure the VLAN ID of the user account.
Syntax	config wac user <username 15> [vlan <vlan_name 32> vlanid <vlanid 1-4094>] clear_vlan]
Description	This command allows you to configure Web-based-function user setting.
Parameters	<i>username</i> – The name of the user account to be changed. <i>vlan</i> – Authentication VLAN name. <i>clear_vlan</i> - To clear the VLAN that is configured previously.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port state:

```
DES-3528:5#config wac user 123 vlan default
Command: config wac user 123 vlan default

Success.

DES-3528:5#
```

config wac virtual_ip

Purpose	Used to configure the WAC virtual ipaddress used to accept authentication requests from an unauthenticated host.
Syntax	config wac virtual_ip <ipaddr>
Description	When the virtual IP is specified, the TCP packet sent to the virtual IP will get a reply. If the virtual IP is enabled, TCP packets sent to the virtual IP or physical IPIF's IP address will both get the a reply. When the virtual IP is set 0.0.0.0, the function of virtual IP is disabled. By default, the virtual IP is 0.0.0.0. The virtual IP will not respond to any ARP request or ICMP packets. To make the function work properly, the virtual IP should not be an existing IP address. It also cannot be located on the existing subnet.
Parameters	<ipaddr> – Specifies the IP address of the virtual IP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WAC virtual IP:

```
DES-3528:5#config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DES-3528:5#
```

show wac_auth_state

Purpose	Used to display the authentication state of a port.
Syntax	show wac_auth_state ports {<portlist>}
Description	<p>Used to display the authentication state for ports.</p> <p>If port 1 is in host-based mode:</p> <p>(1) mac 00-00-00-00-00-01 is authenticated without VLAN assigned (may be the specified target VLAN does not exist or the target VLAN has not been specified), the ID of RX VLAN will be displayed (RX VLAN ID is 4004 in this example).</p> <p>(2) mac 00-00-00-00-00-02 is authenticated with target VLAN assigned, the ID of target VLAN will be displayed (target VLAN ID is 1234 in this example)</p> <p>(3) mac 00-00-00-00-00-03 failed to pass authentication, the VID field will be shown as "-" indicating that packets with SA 00-00-00-00-00-03 will be dropped no matter which VLAN these packets are from.</p> <p>(4) mac 00-00-00-00-00-04 attempts to start authentication, the VID field will be shown as "-" until authentication completed.</p> <p>If port 2 is in port-based mode:</p> <p>(1) mac 00-00-00-00-00-10 is the mac which made port 2 pass authentication, mac address with "(P)" in the end indicates that this authentication is from a port in port-based mode.</p> <p>If port 3 is in port-based mode:</p> <p>(1) mac 00-00-00-00-00-20 attempts to start authentication, mac address with "(P)" in the end indicates the port-based mode authentication.</p> <p>(2) mac 00-00-00-00-00-21 failed to pass authentication, mac address with "(P)" in the end indicates the port-based mode authentication.</p> <p>NOTE : In port-based mode, the VLAN ID field is displayed in the same way as host-based mode</p>
Parameters	<i>ports</i> – Specifies the list of ports whose WAC state will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the WAC authentication state:

```
DES-3528:5# show wac_auth_state ports 1-3
```

```
Command: show wac_auth_state ports 1-3
```

Port	MAC Address	State	VLAN ID	Assigned Priority	Aging Time/ Block Time	Idle Time
1	00-00-00-00-00-01	Authenticated	4004	3	Infinite	40
1	00-00-00-00-00-02	Authenticated	1234	-	Infinite	50
1	00-00-00-00-00-03	Blocked	-	-	60	-
1	00-00-00-00-00-04	Authenticating	-	-	10	-
2	00-00-00-00-00-10(P)	Authenticated	1234	2	1440	20
3	00-00-00-00-00-20(P)	Authenticating	-	-	5	-
3	00-00-00-00-00-21(P)	Blocked	-	-	100	-

```
Total Authenticating Hosts :2
```

```
Total Authenticated Hosts :3
```

```
Total Blocked Hosts :2
```

```
DES-3528:5#
```

create wac user

Purpose	Used to create user account for web-based access control .
Syntax	create wac user <username 15>{[vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
Description	This command allows you to create account for web-base access control. This user account is independent with login user account.
Parameters	<i>username</i> – User account for web-base access control. <i>vlan</i> – Authentication vlan name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a WAC account:

```
DES-3528:5#create wac user 123 vlan default
Command: create wac user 123 vlan default

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

DES-3528:5#
```

delete wac user

Purpose	Used to delete the account for Web-based access control.
Syntax	delete wac user [user <username 15> all_user]
Description	This command allows you to delete an account.
Parameters	<i>username</i> – User account for Web-based access control. <i>all_users</i> – To delete all the users.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a WAC account:

```
DES-3528:5#delete wac user 123
Command: delete wac user 123

Success.

DES-3528:5#
```

show wac

Purpose	Used to display WAC authentication settings.
Syntax	show wac {ports <portlist> all}
Description	This command allows you to display the Web authentication setting.
Parameters	<i>ports</i> – A range of member ports to show the status. <i>all</i> – Will show the status of all the member ports.
Restrictions	None.

Example usage:

To display the WAC state:

```
DES-3528:5#show wac
Command: show wac

Web-Base Access Control
-----
State           : Enable
Method          : Local
Authentication Failover : Disabled
Redirect Path    :
Virtual IP       : 0.0.0.0
Switch HTTP Port : 80 (HTTP)
RADIUS Authorization : Enabled
Local Authorization : Enabled

DES-3528:5#
```

To display WAC ports:

```
DES-3528:5#show wac ports 1-8
Command: show wac ports 1:1-1:8

Port      State      Aging Time      Idle Time      Block Time
-----  -
          (Minutes)    (Minutes)       (Seconds)
-----  -
1:1      Enabled    1440            Infinite       60
1:2      Enabled    1440            Infinite       60
1:3      Enabled    1440            Infinite       60
1:4      Enabled    1440            Infinite       60
1:5      Enabled    1440            Infinite       60
1:6      Enabled    1440            Infinite       60
1:7      Enabled    1440            Infinite       60
1:8      Enabled    1440            Infinite       60

DES-3528:5#
```

show wac user

Purpose	Used to display the user account for web authentication.
Syntax	show wac user
Description	This command allows you to show web authentication account.
Parameters	None.
Restrictions	None.

Example usage:

To show Web authentication account:

```
DES-3528:5#show wac user
Command: show wac user

  Username      Password      VID
  -----
  123           123          1

Total Entries:1

DES-3528:5#
```

clear wac auth_state

Purpose	Used to clear the authentication state of a port.
Syntax	clear wac auth_state ports [<portlist> all] {authenticated authenticating blocked }
Description	This command is used to clear the authentication state of a port. The port will return to an un-authenticated state. All the timers associated with the port will be reset.
Parameters	<p><i><portlist></i> – Specifies the list of ports whose WAC state will be cleared.</p> <p><i>all</i> – Specifies all the ports whose WAC state will be cleared.</p> <p><i>authenticated</i> – Specifies to delete the host in this state.</p> <p><i>authenticating</i> – Specifies to delete the host in this state.</p> <p><i>blocked</i> - Specifies to delete the host in this state.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the WAC authenticated state:

```
DES-3528:5#clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

DES-3528:5#
```

PoE COMMANDS

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

Command	Parameters
config poe system	{units [<unitlist> all]} {power_limit <value 37-370> power_disconnect_method [deny_next_port deny_low_priority_port] }(1)
config poe ports	[all <portlist>] { state [enable disable] [time_range <range_name 32> clear_time_range] priority [critical high low] power_limit [class_0 class_1 class_2 class_3 user_define <value 1000-35000>] } (1)
show poe system	{units <unitlist>}
show poe ports	{ <portlist> }

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

config poe system

Purpose	Used to configure the parameters for the POE system-wise function.
Syntax	config poe system {units [<unitlist> all]} {power_limit <value 37-370> power_disconnect_method [deny_next_port deny_low_priority_port] }(1)
Description	This command is used to configure the parameters for the whole PoE system.
Parameters	<p><i>units</i> - Specifies the units that will be configured. If no specified units, all supported PoE units in the system will be configured.</p> <p><i>power_limit</i> – Configure the power budget for the PoE system. The range which can be specified is determined by the system. Normally, the minimum setting is 37 W and the maximum setting is 370 W. The actual range will depend on power supply capabilities.</p> <p><i>power_disconnect_method</i> – Configure the disconnection method that will be used when the power budget is running out. When the system attempts to supply power to a new port, if the power budget is insufficient to do this, the PoE controller will initiate a port disconnection procedure to prevent overloading the power supply. The controller uses one of the following two ways to perform the disconnection procedure.</p> <p><i>deny_next_port</i> – the port with the highest port number will be denied regardless of its priority.</p> <p>Note that if the disconnect_method is set to deny_next_port, then the power provision will not utilize the system's maximum power. There is a 19W safe margin. That is, when the system has only 19W remaining, this power cannot be utilized.</p> <p><i>deny_low_priority_port</i> – If there are ports that have been supplied power but have a priority lower than the new port, the port with the lowest priority will be disconnected. This process will stop until enough power is released for the new port.</p> <p>Note that if the disconnect_method is set to deny_low_priority_port, then the power provision can utilize the system's maximum power.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the PoE system wide settings:

```
DES-3528P:5# config poe system power_limit 250 power_disconnect_method
deny_low_priority_port
Command: config poe system power_limit 250 power_disconnect_method
deny_low_priority_port
```

Success.

DES-3528P:5#

config poe ports

Purpose	Used to configure the PoE port settings.
Syntax	config poe ports [all <portlist>] { state [enable disable] [time_range <range_name 32> clear_time_range] priority [critical high low] power_limit [class_0 class_1 class_2 class_3 user_define <value 1000-35000>] }(1)
Description	This command is used to configure the PoE port settings.
Parameters	<p><i>portlist</i> – Specifies the list of ports whose setting is under configuration.</p> <p><i>state</i> – When the state is set to disable, power will not be supplied to the powered device connected to this port.</p> <p><i>time_range</i> - Specifies a range of the time to the port set as POE.If time range is configured, the power can only be supplied during the specified period of time.</p> <p><i>Clear_time_range</i> – delete the setting of time range.</p> <p><i>priority</i> – Port priority determines the priority with which the system attempts to supply the power to the ports. There are three levels of priority that can be selected, critical, high, and low. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of the priority will affect the ordering of supplying power. Even if the disconnect_method is set to deny_low_priority_port, priority of the ports will be used by the system to manage and supply power to ports.</p> <p><i>power_limit</i> – Configure the per-port power limit. If a port exceeds its power limit, it will be shut down.</p> <p>Based on 802.3af/at, there are 5 kinds of PD classes;</p> <p>Class 0 – 0.44~12.95W</p> <p>Class 1– 0.44~3.84W</p> <p>Class 2 – 3.84~6.49W</p> <p>Class 3 – 6.49~12.95W</p> <p>Class 4 – 12.95W~29.5W</p> <p>The following is the power limit applied to the port for these five classes. For each class, the power limit is a little more than the power consumption range for the class. This takes the factor of the power loss on cable into account. Thus, the following are the typical values defined by the chip vendor.</p> <p>class_0 – 15400mW</p> <p>class_1 – 4000mW</p> <p>class_2 – 7000mW</p> <p>class_3 – 15400mW</p> <p>User define – 35000mW (only for ports 1~8, but ports 1-8 are only tested up to the 30W mode for the maximum power)</p> <p>As well as these four pre-defined settings, users can directly specify any value ranging from 1000 mW to 35000mW on port 1~8 and 1000mW~15400mW on port 9~24.</p>



NOTE: DES-3528P ports 1~8 can configure PoE up to 35W by configuring the PoE port user define value, but ports 1-8 are only tested up to the 30W mode for the maximum power. All ports can also support 802.3af (1000~15400mW).

config poe ports

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure PoE ports:

```
DES-3528P:5#config poe ports 1-4 state enable priority critical power_limit class_1
Command: config poe ports 1-4 state enable priority critical power_limit class_1

Power limit has been set to 4000 (Class 1 PD upper power limit 3.84W + power loss on
cable)
Success.

DES-3528P:5#config poe ports 5 state enable priority critical power_limit user_define
1000
Command: config poe ports 5 state enable priority critical power_limit user_define
1000

Power limit has been set to 1000
Success.

DES-3528P:5#
```

show poe system

Purpose Used to display the settings and actual values of all PoE functions.

Syntax `show poe system { units <unitlist>}`

Description This command displays the settings and actual values of all PoE functions.

Parameters *units* - Specifies the units that will be displayed.

Restrictions None.

Example usage:

To display all PoE system settings:

```
DES-3528P:5#show poe system
Command: show poe system

PoE System Information
-----
Power Limit           : 250(Watts)
Power Consumption     : 0(Watts)
Power Remained        : 250(Watts)
Power Disconnection Method : Deny Low Priority Port

If Power Disconnection Method is set to deny next port, then the system can not
utilize out of its maximum power capacity. The maximum unused watt is 19W.

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

show poe ports

Purpose	Used to display the settings and actual values of the PoE ports.
Syntax	show poe ports {<portlist>}
Description	This command displays the settings and actual values of the PoE ports.
Parameters	<portlist> – Specifies a list of ports to be displayed. If no parameter is specified, the system will display the status for all ports.
Restrictions	None.

Example usage:

To display all PoE ports:

```
DES-3528P:5#show poe ports 1-6
Command: show poe ports 1-6
```

Port	State	Priority	Power Limit(mW)	Time_Range
	Class	Power(mW)	Voltage(decivolt)	Current(mA)
	Status			
=====				
1	Enabled	Critical	4000 (Class 1)	
	0	0	0	0
	OFF : Interim state during line detection			
2	Enabled	Critical	4000 (Class 1)	
	0	0	0	0
	OFF : Interim state during line detection			
3	Enabled	Critical	4000 (Class 1)	
	0	0	0	0
	OFF : Interim state during line detection			
4	Enabled	Critical	4000 (Class 1)	
	0	0	0	0
	OFF : Interim state during line detection			
5	Enabled	Critical	1000 (User-defined)	
	0	0	0	0
	OFF : Interim state during line detection			
6	Enabled	Low	7000 (User-defined)	
	0	0	0	0
	OFF : Interim state during line detection			

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

PPPOE CIRCUIT ID INSERTION COMMANDS

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]
show pppoe circuit_id_insertion	

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

config pppoe circuit_id_insertion state

Purpose	Used to configure the pppoe circuit id insertion state on the Switch.
Syntax	config pppoe circuit_id_insertion state [enable disable]
Description	When the setting is enabled, the system will insert the circuit ID tag to the received PPPoE discover request and also the request packet if the tag is absent. While enabled it will remove the circuit ID tag from the received PPPoE offer and session confirmation packet. The circuit ID will contain the following information: Client MAC address, switch IP address and port number. The setting is disabled by default.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the pppoe circuit_id_insertion state:

```
DES-3528:5#config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable

Success.

DES-3528:5#
```

show pppoe circuit_id_insertion

Purpose	Used to display the current status of the PPPoE circuit id insertion on the Switch.
Syntax	show pppoe circuit_id_insertion
Description	None.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the pppoe circuit_id_insertion state:

```
DES-3528:5#show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Status: Enabled

DES-3528:5#
```

DNS RELAY COMMANDS

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

Command	Parameters
config dnsm	[[primary secondary] nameserver <ipaddr> [add delete] static <domain_name 32> <ipaddr>]
enable dnsm	{[cache static]}
disable dnsm	{[cache static]}
show dnsm	{static}

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

config dnsm

Purpose	Used to add or delete a static entry in the DNS resolution table
Syntax	config dnsm [[primary secondary] nameserver <ipaddr> [add delete] static <domain_name 32> <ipaddr>]
Description	This command is used to add or delete a static entry in the DNS resolution table
Parameters	<p><i>primary</i> - When both primary and secondary server exist, the primary server will be used.</p> <p><i>secondary</i> - When the primary server does not exist, the secondary server will be used.</p> <p><i>nameserver <ipaddr></i> - Specifies the IP address of primary or secondary name server.</p> <p><i><domain_name 32><ipaddr></i> - Specifies the name of the server and IP address of the corresponding in DNS Static Table in DNS server.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DNS relay:

```
DES-3528:5#config dnsm primary nameserver 192.168.1.1
Command: config dnsm primary nameserver 192.168.1.1
```

Success.

```
DES-3528:5#
```

enable dnsm

Purpose	Used to enable DNS relay function.
Syntax	enable dnsm {[cache static]}
Description	This command is used to enable DNS relay function.
Parameters	<p><i>cache</i> - The buffer cache which records the name of the server and IP address of the corresponding.</p> <p><i>static</i> - The DNS Static Table in DNS server with the name of the server and the corresponding IP address.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the DNS relay:

```
DES-3528:5#enable dnsr cache
Command: enable dnsr cache

Success.

DES-3528:5#
```

disable dnsr

Purpose	Used to disable DNS relay function.
Syntax	disable dnsr {[cache static]}
Description	This command is used to disable DNS relay function.
Parameters	<i>cache</i> - The buffer cache which records the name of the server and IP address of the corresponding. <i>static</i> - The DNS Static Table in DNS server with the name of the server and IP address of the corresponding.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the DNS relay:

```
DES-3528:5#disable dnsr cache
Command: disable dnsr cache

Success.

DES-3528:5#
```

show dnsr

Purpose	Used to display the current DNS relay static table.
Syntax	show dnsr {static}
Description	This command is used to display the current DNS relay static table.
Parameters	{ <i>static</i> } - The DNS Static Table in DNS server with the name of the server and IP address.
Restrictions	None

Example usage:

To display the DNS relay:

```
DES-3528:5#show dnsr
```

```
Command: show dnsr
```

```
DNSR Status           : Enabled  
Primary Name Server   : 192.168.1.1  
Secondary Name Server : 0.0.0.0  
DNSR Cache Status     : Enabled  
DNSR Static Table Status : Disabled
```

```
DNS Relay Static Table
```

Domain Name	IP Address
-----	-----
tt.cn.alphanetworks.com	192.168.1.1

```
Total Entries: 1
```

POLICY ROUTE COMMANDS

The Policy Route commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create policy_route name	<policyroute_name 32>
config policy_route name	<policyroute_name 32>acl profile_id <value 1-14> access_id <value 1-128>nexthop <ipaddr> state [enable disable]
delete policy_route name	<policyroute_name 32>
show policy_route	

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

create policy_route name

Purpose	Used to add policy route rule.
Syntax	create policy_route name <policyroute_name 32>
Description	This command allows you to create policy route and define this rule name. <ul style="list-style-type: none"> The ACL rule that is linked to the policy route command could not be deleted via ACL command.
Parameters	<policyroute_name 32> – Specifies the name of police rule. Max length is 32 character.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a policy route:

```
DES-3528:5# create policy_route name engineer
Command: create policy_route name engineer

Success.

DES-3528:5#
```

config policy_route

Purpose	Used to config policy route rule.
Syntax	config policy_route name <policyroute_name 32>acl profile_id <value 1-14> access_id <value 1-128>nexthop <ipaddr> state [enable disable]
Description	<p>This command allows you to config the different fields for a policy route entry. You can set the state of a policy route to enable or disable.</p> <ul style="list-style-type: none"> • Create a ACL rule. If no acl rule exists, system will show an error message. • If any ACL rule action is dropped, the packet will not be forwarded, and not implement policy route. • Packets pass from policy route, its TTL will decrease 1 • If user delete a ACL rule that is linked a policy rule, system will pop error message.
Parameters	<p><i>name</i> – Specifies the name of police rule. <i>profile_id</i> – Specifies the ACL profile ID. <i>access_id</i> – Specifies the ACL access ID. <i>nexthop</i> – Specifies the next hop IP address. <i>state</i> – Enables or disables the rule.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config a policy route:

```
DES-3528:5# config policy_route name engineer acl profile_id 1 access_id 1 nexthop
20.1.1.100 state enable
Command: config policy_route name engineer acl profile_id 1 access_id 1 nexthop 20.1.1.100
state enable

Success.

DES-3528:5#
```

delete policy_route

Purpose	Used to delete policy route rule.
Syntax	delete policy_route name<policyroute_name 32>
Description	This command is used to delete policy route rule.
Parameters	<policyroute_name 32> – Specifies the name of police rule.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a policy route:

```
DES-3528:5# delete policy_route name engineer
Command: delete policy_route name engineer

Success.

DES-3528:5#
```

show policy_route

Purpose	Used to display policy route rule.
Syntax	show policy_route
Description	This command is used to display policy route rule.
Parameters	None.
Restrictions	None.

Example usage:

To show available policy routes:

```
DES-3528:5# show policy_route
Command: show policy_route

Policy Routing Table

Name           Profile ID  Access ID  Nexthop           State
-----
engineer       1           1          20.1.1.100       Enabled

Total Entries : 1

DES-3528:5#
```

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.



NOTE: The BPDU Attack Protection commands and STP Function commands are mutually exclusively. Therefore, 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

Command	Parameters
config bpdu_protection ports	[<portlist> all] {state [enable disable] mode [drop block disable]} (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.

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 disable]} (1)
Description	This command is used to setup the BPDU Attack Protection function for the ports on the switch.
Parameters	<p><i>portlist</i> – Specifies a range of ports to be configured.</p> <p><i>all</i> – In order to set all ports in the system, you may use the “all” parameter.</p> <p><i>state</i> – Specifies the state of BPDU Attack Protection. The default state is disable</p> <p><i>enable</i> – Enables the port or ports for BPDU Attack Protection.</p> <p><i>disable</i> – Disables the port or ports for BPDU Attack Protection.</p> <p><i>mode</i> – Specifies the BPDU Attack Protection mode. The default mode is drop.</p> <p><i>drop</i> – Will drop all RX BPDU packets when the port enters under_attack state.</p> <p><i>block</i> – Will drop all RX packets (include BPDU and normal packets) when the port enters under_attack state.</p> <p><i>disable</i> – Will shut down the port when the port enters under_attack state.</p>



NOTE: The RX BPDU Attack Protection takes affect only when the port enters under_attack state while in drop and block mode.

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

Example usage:

To configure the BPDU Attack Protection mode to drop for port 1:

```
DES-3528:5#config bpdu_protection ports 1 state enable mode drop
Command: config bpdu_protection ports 1 state enable mode drop

Success.

DES-3528:5#
```

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 the port first and then enable the port.
Parameters	<p><i>recover_timer</i> – Specifies the recover_timer. The default value of recovery timer is 60.</p> <p><i>infinite</i> – The port will not be auto recovered.</p> <p><i><sec 60-1000000></i> – The timer (in seconds) used by the auto-recovery mechanism to recover the port. The valid range is 60 to 1000000.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the BPDU Attack Protection recovery timer to 120 seconds for the entire switch:

```
DES-3528:5#config bpdu_protection recovery_timer 120
Command: config bpdu_protection recovery_timer 120

Success.

DES-3528:5#
```

config bpdu_protection

Purpose	Used to configure the trap or log state of BPDU Attack Protection.
Syntax	config bpdu_protection [trap log] [none attack_detected attack_cleared both]
Description	This command is used to configure trap or log state for BPDU Attack Protection function.
Parameters	<p><i>trap</i> – Specifies the trap state. The default state is both trap and log.</p> <p><i>log</i> – Specifies the log state. The default state is both trap and log.</p> <p><i>none</i> – Specifies that events will not be logged or trapped for both cases.</p> <p><i>attack_detected</i> – Specifies events will be logged or trapped when a BPDU attack is detected.</p> <p><i>attack_cleared</i> – Specifies that events will be logged or trapped when the BPDU attack is cleared.</p> <p><i>both</i> – Specifies that events will be logged or trapped for both cases.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the BPDU Attack Protection trap state as both for the entire switch:

```
DES-3528:5#config bpdu_protection trap both
Command: config bpdu_protection trap both

Success.

DES-3528:5#
```

enable bpdu_protection

Purpose	Used to enable BPDU Attack Protection globally.
Syntax	enable bpdu_protection
Description	This command allows the BPDU Attack Protection to be globally enabled on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the BPDU Attack Protection function globally for the entire switch:

```
DES-3528:5#enable bpdu_protection
Command: enable bpdu_protection

Success.

DES-3528:5#
```

disable bpdu_protection

Purpose	Used to disable BPDU Attack Protection globally.
Syntax	disable bpdu_protection
Description	This command allows BPDU Attack Protection to be globally disabled on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the BPDU Attack Protection function globally for the entire switch:

```
DES-3528:5#disable bpdu_protection
Command: disable bpdu_protection

Success.

DES-3528:5#
```


show bpdu_protection

Purpose	Used to display BPDU Attack Protection status.
Syntax	show bpdu_protection {ports {<portlist>}}
Description	This command is used to display BPDU Attack Protection global configuration or per port configuration and current status.
Parameters	portlist – Specifies a range of ports to be displayed.
Restrictions	None.

Example usage:

To display the BPDU Attack Protection status of the entire switch:

```
DES-3528:5#show bpdu_protection
Command: show bpdu_protection

BPDU Protection Global Settings
-----
BPDU Protection Status           : Enabled
BPDU Protection Recover Time     : 120 seconds
BPDU Protection Trap Status      : Both
BPDU Protection Log Status       : Both

DES-3528:5#
```

To display the BPDU Attack Protection status for ports 1-4 of the Switch:

```
DES-3528:5#show bpdu_protection ports 1-4
Command: show bpdu_protection ports 1-4

Port  State      Mode      Status
-----
1     Enabled      Drop      Normal
2     Disabled     Drop      Normal
3     Disabled     Drop      Normal
4     Disabled     Drop      Normal

DES-3528:5#
```


ETHERNET OAM COMMANDS

The 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	[<portlist> all] [mode [active passive] state [enable disable] link_monitor [error_symbol { threshold <range 0 - 4294967295> window <millisecond> notify_state [enable disable]}(1) error_frame { threshold <range 0 - 4294967295> window <millisecond> notify_state [enable disable]}(1) error_frame_seconds { threshold <range 0 - 4294967295> window <millisecond> notify_state [enable disable]}(1) error_frame_period { threshold <range 0 - 4294967295> window <number> notify_state [enable disable]}(1)] critical_link_event [dying_gasp critical_event] notify_state [enable disable] remote_loopback [start stop] received_remote_loopback [process ignore]]
show ethernet_oam ports	{<portlist>} [status configuration statistics event_log {index <value_list>}]
clear ethernet_oam ports	[<portlist> all] [event_log statistics]

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

config ethernet_oam ports mode

Purpose	Used to configure Ethernet OAM mode.
Syntax	config ethernet_oam ports [<portlist> all] mode [active passive]
Description	<p>This command is used to configure ports Ethernet OAM to operate in active or passive mode. The following two actions are allowed by ports in active mode, but disallowed by ports in passive mode.</p> <p>Initiate OAM discovery and Start or stop remote loop-back.</p>
	 <p>NOTE: When a port is OAM-enabled, changing the OAM mode will cause the OAM discovery to be re-started.</p>
Parameters	<p><i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify all ports.</p> <p><i>mode</i> – Specifies to operate in either active mode or passive mode. The default mode is active.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 1 to OAM mode to passive:

```
DES-3528:5#config ethernet_oam ports 1 mode passive
```

```
Command: config ethernet_oam ports 1 mode passive
```

```
Success.
```

```
DES-3528:5#
```

config ethernet_oam ports state

Purpose	Used to enable or disable Ethernet OAM.
Syntax	config ethernet_oam ports [<portlist> all] state [enable disable]
Description	This command used to enable or disable the port's Ethernet OAM function. Enabling a port's OAM will cause the port to start OAM discovery. If a port is active, it initiates the discovery otherwise it reacts only to the discovery received from its peer. Disabling a port's OAM will cause the port to send out a dying gasp event to the peer and then disconnect the established OAM link.
Parameters	<i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify all ports. <i>state</i> – Specifies to enable or disable the OAM function. The default state is disable.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable Ethernet OAM on port 1:

```
DES-3528:5#config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.
DES-3528:5#
```

config ethernet_oam ports link_monitor error_symbol

Purpose	Used to configure Ethernet OAM link monitoring error symbols.
Syntax	config ethernet_oam ports [<portlist> all] link_monitor error_symbol{ threshold <range 0 - 4294967295> window <millisecond> notify_state [enable disable]}(1)
Description	This command is used to configure ports Ethernet OAM link monitoring error symbols. The link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of symbol errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error symbol period event to notify the remote OAM peer.
Parameters	<i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify all ports. <i>threshold</i> – Specifies the number of symbol errors in the period that is required to be equal to or greater than in order for the event to be generated. The range is from 0 to 4294967295. The default value of threshold is 1 symbol error. <i>window</i> – The range is 1000 to 60000 ms. The default value is 1000ms. <i>notify_state</i> – Specifies to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DES-3528:5#config ethernet_oam ports 1 link_monitor error_symbol threshold 2 window
1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_symbol threshold 2 window
1000 notify_state enable

Success.

DES-3528:5#
```

config ethernet_oam ports link_monitor error_frame

Purpose	Used to configure Ethernet OAM link monitoring error frame
Syntax	config ethernet_oam ports [<portlist> all] link_monitor error_frame{ threshold <range 0 - 4294967295> window <millisecond> notify_state [enable disable]}(1)
Description	The command used to configure ports Ethernet OAM link monitoring error frames. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counter on the number of frame errors as well as the number of coding symbol errors. When the number of frame errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame event to notify the remote OAM peer.
Parameters	<i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify all ports. <i>threshold</i> – Specifies the number of frame errors in the period that are required to be equal to or greater than in order for the event to be generated. The range is from 0 to 4294967295. The default value of threshold is 1 frame error. <i>window</i> – The range is 1000 to 60000 ms. The default value is 1000ms. <i>notify_state</i> – Specifies to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator and Operator-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-3528:5#config ethernet_oam ports 1 link_monitor error_frame threshold 2 window 1000 notify_state enable
```

```
Command: config ethernet_oam ports 1 link_monitor error_frame threshold 2 window 1000 notify_state enable
```

Success.

```
DES-3528:5#
```

config ethernet_oam ports link_monitor error_frame_seconds

Purpose	Used to configure Ethernet OAM link monitoring error frame seconds.
Syntax	config ethernet_oam ports [<portlist> all] link_monitor error_frame_seconds { threshold <range 0 - 4294967295> window <millisecond> notify_state [enable disable]}(1)
Description	This command is used to configure ports Ethernet OAM link monitoring error frame seconds. An error frame second is a 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 counter on the number of frame errors as well as the number of coding symbol errors. When the number of error frame seconds are equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame second summary event to notify the remote OAM.
Parameters	<i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify all ports. <i>threshold</i> – Specifies the number of error frame seconds in the period that are required to be equal to or greater than in order for the event to be generated. The range is from 0 to 4294967295. The default value of threshold is 1 error frame second. <i>window</i> – Specifies the period of error frame seconds summary event. The range is 10000ms-900000ms and the default value is 60000 ms. <i>notify_state</i> – Specifies to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator and Operator-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-3528:5#config ethernet_oam ports 1 link_monitor error_frame_seconds threshold 2
window 10000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_seconds threshold 2
window 10000 notify_state enable

Success.

DES-3528:5#
```

config ethernet_oam ports link_monitor error_frame_period

Purpose	Used to configure the Ethernet OAM link monitoring error frame period.
Syntax	config ethernet_oam ports [<portlist> all] link_monitor error_frame_period{ threshold <range 0 - 4294967295> window <millisecond> notify_state [enable disable]}(1)
Description	This command is used to configure ports Ethernet OAM link monitoring error frame period. 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 error frames are 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.
Parameters	<p><i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify <i>all ports</i>.</p> <p><i>threshold</i> – Specifies the number of error frame seconds in the period that are required to be equal to or greater than in order for the event to be generated. The range is from 0 to 4294967295. The default value of the threshold is 1 error frame.</p> <p><i>window</i> – Specifies the period of the error frame period event. The period is specified by a number of received frames. The range for this setting is 148 810 to 100 000 000. The default value is 1 488 100 frames.</p> <p><i>notify_state</i> – Specifies to enable or disable the event notification. The default state is enable.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the errored frame threshold to 10 and period to 1000000 for port 1 of unit 1:

```
DES-3528:5#config ethernet_oam ports 1 link_monitor error_frame_period threshold 10
window 1000000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_period threshold 10
window 1000000 notify_state enable

Success.

DES-3528:5#
```

config ethernet_oam ports critical_link_event

Purpose	Used to configure Ethernet OAM critical link event.
Syntax	config ethernet_oam ports [<portlist> all] critical_link_event [dying_gasp critical_event] notify_state [enable disable]
Description	This command is used to configure the capability of Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event.
Parameters	<p><i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify all ports.</p> <p><i>dying_gasp</i> – An unrecoverable local failure condition has occurred.</p> <p><i>critical_event</i> – An unspecified critical event has occurred.</p> <p><i>notify_state</i> – Specifies to enable or disable the event notification. The default state is enable.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure dying_gasp event for port 1:

```
DES-3528:5#config ethernet_oam ports 1 critical_link_event dying_gasp notify_state
enable
Command: config ethernet_oam ports 1 critical_link_event dying_gasp notify_state
enable

Success.

DES-3528:5#
```

config ethernet_oam ports remote_loopback

Purpose	Used to start or stop Ethernet OAM remote loop-back .
Syntax	config ethernet_oam ports [<portlist> all] remote_loopback [start stop]
Description	<p>This command is used to start or stop the remote peer to enter the Ethernet OAM remote loop-back mode.</p> <p>To start the remote peer to enter the remote loop-back mode, you must ensure the port is in active mode and the OAM connection is established. If the local client is already in remote loop-back mode, then it cannot apply this command.</p>
Parameters	<p><i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify all ports.</p> <p><i>remote_loopback</i> – If start is specified, it will request the peer to change to the remote loop-back mode. If stop is specified, it will request the peer to change to the normal operation mode.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To start remote loop-back on port 1:

```
DES-3528:5#config ethernet_oam ports 1 remote_loopback stop
Command: config ethernet_oam ports 1 remote_loopback stop

Success.

DES-3528:5#
```

config ethernet_oam ports received_remote_loopback

Purpose	Used to configure the method to process the received Ethernet OAM remote loop-back command.
Syntax	config ethernet_oam ports [<portlist> all] received_remote_loopback [process ignore]
Description	This command is used to configure the client to process or to ignore the received Ethernet OAM remote loop-back command. In remote loop-back mode, all user traffic will not be processed. Ignoring received remote loop-back command will prevent the port from entering remote loop-back mode.
Parameters	<i>portlist</i> – Specifies a range of ports to be configured. Use <i>all</i> to specify all ports. <i>received_remote_loopback</i> – Specifies whether to process or to ignore the received Ethernet OAM remote loop-back command. The default method is "ignore".
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the method of processing the received remote loop-back command as "process" on port 1:

```
DES-3528:5#config ethernet_oam ports 1 received_remote_loopback process
Command: config ethernet_oam ports 1 received_remote_loopback process
```

Success.

```
DES-3528:5#
```

show ethernet_oam ports status

Purpose	Used to show primary controls and status information for Ethernet OAM.
Syntax	show ethernet_oam ports {<portlist>} status
Description	This command is used to show primary controls and status information for Ethernet OAM on specified ports. The information includes: (1) OAM administration status: enabled or disabled (2) OAM operation status. See below values: Disable: OAM is disabled on this port LinkFault: The link has detected a fault and is transmitting OAMPDUs with a link fault indication. PassiveWait: The port is passive and is waiting to see if the peer device is OAM capable. ActiveSendLocal: The port is active and is sending local information SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer. SendLocalAndRemoteOk: The local device agrees the OAM peer entity. PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity. PeeringRemotelyRejected: The remote OAM entity rejects the local device. Operational: The local OAM entity learns that both it and the remote OAM entity have accepted the peering. NonOperHalfDuplex: Since Ethernet OAM functions are not designed to work completely over half-duplex ports. 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

show ethernet_oam ports status

the latest OAMPDU sent by the OAM entity. The config revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed.

OAM mode change.

(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 loop-back 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

At present, only loop-back and link monitoring are supported.

Parameters *portlist* – Specifies a range of ports to display.

Restrictions None

Example usage:

To show OAM control and status information on port 1-2:

```
DES-3528:5#show ethernet_oam ports 1-2 status
```

```
Command: show ethernet_oam ports 1-2 status
```

```
Port 1
```

```
Local Client
```

```
-----
OAM                : Enabled
Mode               : Passive
Max OAMPDU         : 1518 Bytes
Remote Loopback    : Support
Unidirection       : Not Supported
Link Monitoring     : Support
Variable Request    : Not Supported
PDU Revision       : 1
Operation Status   : LinkFault
Loopback Status    : No Loopback
```

```
There is no peer entry information exist !
```

```
Port 2
```

```
Local Client
```

```
-----
OAM                : Disabled
Mode               : Active
Max OAMPDU         : 1518 Bytes
```

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


show ethernet_oam ports configuration

Purpose	Used to display Ethernet OAM configuration.
Syntax	show ethernet_oam ports {<portlist>} configuration
Description	This command is used to show port's Ethernet OAM configurations.
Parameters	<i>portlist</i> – Specifies a range of ports to display.
Restrictions	None.

Example usage:

To show Ethernet OAM configuration on port 1-2:

```
DES-3528:5#show ethernet_oam ports 1-2 configuration
Command: show ethernet_oam ports 1-2 configuration

Port 1
-----
OAM                : Enabled
Mode               : Passive
Dying Gasp         : Enabled
Critical Event     : Enabled
Remote Loopback OAMPDU : Processed

Symbol Error
  Notify State     : Enabled
  Window:         : 1000 milliseconds
  Threshold       : 2 Errored Symbol

Frame Error
  Notify State     : Enabled
  Window:         : 1000 milliseconds
  Threshold       : 2 Errored Frame

Frame Period Error
  Notify State     : Enabled
  Window:         : 1000000 Frames
  Threshold       : 10 Errored Frame

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

show ethernet_oam ports statistics

Purpose	Used to show Ethernet OAM statistics.
Syntax	show ethernet_oam ports {<portlist>} statistics
Description	This command is used to show ports Ethernet OAM statistics information.
Parameters	<i>portlist</i> – Specifies a range of ports to display.
Restrictions	None.

Example usage:

To show port 1 OAM statistics:

```
DES-3528:5#show ethernet_oam ports 1 statistics
```

```
Command: show ethernet_oam ports 1 statistics
```

```
Port 1
```

```
-----
Information OAMPDU Tx           : 0
Information OAMPDU Rx           : 0
Unique Event Notification OAMPDU Tx : 0
Unique Event Notification OAMPDU Rx : 0
Duplicate Event Notification OAMPDU Tx: 0
Duplicate Event Notification OAMPDU Rx: 0
Loopback Control OAMPDU Tx      : 0
Loopback Control OAMPDU Rx      : 0
Variable Request OAMPDU Tx      : 0
Variable Request OAMPDU Rx      : 0
Variable Response OAMPDU Tx     : 0
Variable Response OAMPDU Rx     : 0
Organization Specific OAMPDU Tx : 0
Organization Specific OAMPDU Rx : 0
Unsupported OAMPDU Tx           : 0
Unsupported OAMPDU Rx           : 0
Frames Lost Due To OAM          : 0
```

```
DES-3528:5#
```

show ethernet_oam event_log

Purpose	Used to show the Ethernet OAM event log.
Syntax	show ethernet_oam {<portlist>} event_log {index <value_list> }
Description	This command is used to show 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. You can specify an index to show a range of events.
Parameters	<i>portlist</i> – Specifies a range of ports to display. <i>index</i> – Specifies an index range to display.
Restrictions	None.

Example usage:

To show port 1 external OAM event:

```
DES-3528:5#show ethernet_oam ports 1 event_log
```

```
Command: show ethernet_oam ports 1 event_log
```

```
Port 1
```

```
-----
```

Event Listing

Index	Type	Location	Time Stamp
-----	-----	-----	-----

Local Event Statistics

Error Symbol Event	: 0
Error Frame Event	: 0
Error Frame Period Event	: 0
Errored Frame Seconds Event	: 0
Dying Gasp	: 0
Critical Event	: 0

Remote Event Statistics

Error Symbol Event	: 0
Error Frame Event	: 0
Error Frame Period Event	: 0
Errored Frame Seconds Event	: 0
Dying Gasp	: 0
Critical Event	: 0

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

clear ethernet_oam ports statistics

Purpose Used to clear Ethernet OAM statistics.

Syntax `clear ethernet_oam ports [<portlist> | all] statistics`

Description This command is used to clear ports Ethernet OAM statistics information.

Parameters *portlist* – Specifies a range of ports to clear the statistics.

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

Example usage:

To clear port 1 OAM statistics:

```
DES-3528:5#clear ethernet_oam ports 1 statistics
```

```
Command: clear ethernet_oam ports 1 statistics
```

```
Success.
```

```
DES-3528:5#
```

clear ethernet_oam ports event_log

Purpose	Used to clear Ethernet OAM event log
Syntax	clear ethernet_oam ports [<portlist> all] event_log
Description	This command is used to clear ports Ethernet OAM event log information.
Parameters	<i>portlist</i> – Specifies a range of ports to clear the event log.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear port 1 OAM event:

```
DES-3528:5#clear ethernet_oam ports 1 event_log
```

```
Command: clear ethernet_oam ports 1 event_log
```

```
Success.
```

```
DES-3528:5#
```

DHCP SERVER COMMANDS

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

Command	Parameters
create dhcp excluded_address	begin_address <ipaddr> end_address <ipaddr>
delete dhcp excluded_address	[begin_address <ipaddr> end_address <ipaddr> all]
show dhcp excluded_address	
create dhcp pool	<pool_name 12>
delete dhcp pool	[<pool_name 12> all]
show dhcp pool	{ <pool_name 12> }
config dhcp pool network_addr	<pool_name 12> <network_address>
config dhcp pool domain_name	<pool_name 12> {<domain_name 64>}
config dhcp pool dns_server	<pool_name 12> {<ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool netbios_name_server	<pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool netbios_node_type	<pool_name 12> [broadcast peer_to_peer mixed hybrid]
config dhcp pool default_router	<pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool lease	<pool_name 12> [<day 0-365> <hour 0-23><minute 0-59> infinite]
config dhcp pool boot_file	<pool_name 12> {<file_name 64>}
config dhcp pool next_server	<pool_name 12> {< ipaddr>}
create dhcp pool manual_binding	<pool_name 12> < ipaddr> hardware_address <macaddr> {type [Ethernet IEEE802]}
delete dhcp pool manual_binding	<pool_name 12> [<ipaddr> all]
show dhcp pool manual_binding	{<pool_name 12>}
config dhcp ping_packets	<number 0-10>
config dhcp ping_timeout	<millisecond 10-2000>
clear dhcp binding	[<pool_name 12> [<ipaddr> all] all]
show dhcp binding	{<pool_name 12>}
enable dhcp_server	
disable dhcp_server	
show dhcp_server	
show dhcp conflict_ip	{<ipaddr>}
clear dhcp conflict_ip	[<ipaddr> all]

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

create dhcp excluded_address

Purpose	Used to specify the IP addresses that the DHCP server will not assign to DHCP client.
Syntax	create dhcp excluded_address begin_address < ipaddr > end_address < ipaddr >
Description	The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. This command is used to specify the IP address that the DHCP server should not assign to clients. This command can be used multiple times in order to define multiple groups of excluded addresses.
Parameters	<ipaddr> – Specifies the beginning and end of the IP address range.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the IP address that the DHCP server should not assign to clients:

```
DES-3528:5#create dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10
Command: create dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10

Success.

DES-3528:5#
```

delete dhcp excluded_address

Purpose	Used to specify the IP addresses that the DHCP server will not assign to DHCP client to be deleted.
Syntax	delete dhcp excluded_address [begin_address < ipaddr > end_address < ipaddr > all]
Description	The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. This command is used to specify the IP address that the DHCP server should not assign to clients to be deleted.
Parameters	<ipaddr> – Specifies the beginning and end of the IP address range.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the IP address that the DHCP server should not assign to clients:

```
DES-3528:5#delete dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10
Command: delete dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10

Success.

DES-3528:5#
```

show dhcp excluded_address

Purpose	Used to display the groups of IP addresses which are excluded from the legal assigned IP address.
Syntax	show dhcp excluded_address
Description	This command shows the groups of IP addresses which are excluded from the legal assigned IP address.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the DHCP excluded addresses:

```
DES-3528:5#show dhcp excluded_address
```

```
Command: show dhcp excluded_address
```

Index	Begin Address	End Address
----	-----	-----
1	10.10.10.1	10.10.10.10

```
Total Entries: 1
```

```
DES-3528:5#
```

create dhcp pool

Purpose	Used to create a DHCP pool.
Syntax	create dhcp pool <pool name 12>
Description	A DHCP pool is created by specifying a name. After you create a DHCP pool, use other DHCP pool configuration commands to configure parameters for the pool. The maximum number of pools that can be configured is 4.
Parameters	<pool name 12> – Specifies the name of the pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create DHCP pool entry:

```
DES-3528:5#create dhcp pool accounting
```

```
Command: create dhcp pool accounting
```

```
Success.
```

```
DES-3528:5#
```

delete dhcp pool

Purpose	Used to delete a DHCP pool entry.
Syntax	delete dhcp pool [<pool name 12> all]
Description	This command is used to delete a previously created DHCP pool entry.
Parameters	<pool name 12> – Specifies the name of the pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a DHCP pool entry:

```
DES-3528:5#delete dhcp pool accounting
Command: delete dhcp pool accounting

Success.

DES-3528:5#
```

config dhcp pool network_addr

Purpose	Used to specify the network for the DHCP pool.
Syntax	config dhcp pool network_addr <pool_name 12> <network_address>
Description	<p>This command Specifies the network for the DHCP pool. The addresses in the network are free to be assigned to the DHCP client. The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).</p> <p>When the DHCP server receives a request from the client, the server will automatically find a pool to allocate the address. If the request is relayed to the server by the intermediate device, the server will match the gateway IP address carried in the packet against the network of each DHCP pool. The pool which has the longest match will be selected.</p> <p>If the request packet is not through relay, then the server will match the IP address of the IPIF that receives the request packet against the network of each DHCP pool.</p>
Parameters	<p><pool name 12> – Specifies the name of the pool.</p> <p><network address> – Specifies the IP address that the DHCP server may assign to clients.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the address range of the DHCP address pool:

```
DES-3528:5#config dhcp pool network_addr accounting 10.10.10.0/24
Command: config dhcp pool network_addr accounting 10.10.10.0/24

Success.

DES-3528:5#
```


config dhcp pool domain_name

Purpose	Used to specify the domain name for the client if the server allocates the address for the client from this pool.
Syntax	config dhcp pool domain_name <pool_name 12> {<domain_name 64>}
Description	The domain name configured here will be used as the default domain name by the client. By default, the domain name is empty. If the domain name is empty, the domain name information will not be provided to the client .
Parameters	<pool name 12> – Specifies the name of the pool. <domain name 64> – Specifies the domain name of the client.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the domain name option of the DHCP pool:

```
DES-3528:5#config dhcp pool domain_name accounting 10.10.10.0/24
Command: config dhcp pool domain_name accounting 10.10.10.0/24

Success.

DES-3528:5#
```

config dhcp pool dns_server

Purpose	Used to specify the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified in one command line.
Syntax	config dhcp pool dns_server <pool_name 12> {<ipaddr>} {< ipaddr>} {< ipaddr>}
Description	If a DNS server is not specified, the DNS server information will not be provided to the client. If this command is entered twice in the same pool, the second command will overwrite the first command.
Parameters	<pool name 12> – Specifies the name of the pool. <ipaddr> – Specifies the IP address of the DNS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DNS server's IP address:

```
DES-3528:5#config dhcp pool dns_server accounting 10.10.10.1
Command: config dhcp pool dns_server accounting 10.10.10.1

Success.

DES-3528:5#
```

config dhcp pool netbios_name_server

Purpose	Used to specify the NetBIOS WINS server that is available to a Microsoft DHCP client. Up to three IP addresses can be specified in one command line.
Syntax	config dhcp pool netbios_name_server <pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}
Description	Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks. If the name of the netbios server is not specified, the netbios name server information will not be provided to the client. If this commands are entered twice for the same pool, the second command will overwrite the first command.
Parameters	<pool name 12> – Specifies the name of the pool. <ipaddr> – Specifies the IP address of the WINS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WINS Server's IP address:

```
DES-3528:5#config dhcp pool netbios_name_server accounting 10.10.10.1
Command: config dhcp pool netbios_name_server accounting 10.10.10.1

Success.

DES-3528:5#
```

config dhcp pool netbios_node_type

Purpose	Used to specify the NetBIOS node type for a Microsoft DHCP client.
Syntax	config dhcp pool netbios_node_type <pool_name 12> [broadcast peer_to_peer mixed hybrid]
Description	The NetBIOS node type for Microsoft DHCP clients can be one of four settings: broadcast, peer-to-peer, mixed, or hybrid. This command is used to configure NetBIOS over a TCP/IP device. By default, NetBIOS node type is broadcast.
Parameters	<pool name 12> – Specifies the name of the pool. <node type> – Specifies the NetBIOS node type for a Microsoft DHCP client.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the NetBIOS node type:

```
DES-3528:5#config dhcp pool netbios_node_type accounting hybrid
Command: config dhcp pool netbios_node_type accounting hybrid

Success.

DES-3528:5#
```

config dhcp pool default_router

Purpose	Used to specify the IP address of the default router for a DHCP client. Up to three IP addresses can be specified in one command line.
Syntax	config dhcp pool default_router <pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}
Description	After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client. If the default_router is not specified, the default router information will not be provided to the client. If this command is entered twice in the same pool, the second command will overwrite the first command.
Parameters	<pool name 12> – Specifies the name of the pool. <ipaddr> – Specifies the IP address of the default router.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the default router:

```
DES-3528:5#config dhcp pool default_router accounting 10.10.10.1
Command: config dhcp pool default_router accounting 10.10.10.1

Success.

DES-3528:5#
```

config dhcp pool lease

Purpose	Used to specify the duration of the lease.
Syntax	config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23><minute 0-59> infinite]
Description	By default, each IP address assigned by a DHCP server comes with a one-day lease, which is the amount of time that the address is valid.
Parameters	<pool_name 12> – Specifies the name of the pool. <day 0-365> – Specifies the days of lease. <hour 0-23> – Specifies the hours of the lease. <minute 0-59> – Specifies the minutes of the lease infinite – Specifies that the lease will be infinite.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the lease of a pool:

```
DES-3528:5#config dhcp pool lease accounting infinite
Command: config dhcp pool lease accounting infinite

Success.

DES-3528:5#
```

config dhcp pool boot_file

Purpose	Used to specify the name of the file that is used as a boot image.
Syntax	config dhcp pool boot_file <pool_name 12> {<file_name 64>}
Description	<p>The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load.</p> <p>If this command is entered twice for the same pool, the second command will overwrite the first command.</p> <p>If the boot file is not specified, the boot_file information will not be provided to the client .</p>
Parameters	<p><pool_name 12> – Specifies the name of the pool.</p> <p><file_name 64> – Specifies the file name of the boot image.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the boot file:

```
DES-3528:5#config dhcp pool boot_file accounting boot.had
Command: config dhcp pool boot_file accounting boot.had

Success.

DES-3528:5#
```

config dhcp pool next_server

Purpose	Used to specify the next server to be used in the DHCP client boot process.
Syntax	config dhcp pool next_server <pool_name 12> {< ipaddr>}
Description	<p>The next server used by the DHCP client boot process is typically a TFTP server. If the next server information is not specified, it will not be provided to the client. If this command is entered twice for the same pool, the second command will overwrite the first command.</p> <p>It is allowed to specify next_server but not specify the boot file, or specify the boot file but not specify the next_server.</p>
Parameters	<p><pool_name 12> – Specifies the name of the pool.</p> <p><ipaddr> – Specifies the IP address of the next server.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the next server:

```
DES-3528:5#config dhcp pool next_server accounting 192.169.0.1
Command: config dhcp pool next_server accounting 192.169.0.1

Success.

DES-3528:5#
```

config dhcp ping_packets

Purpose	Used to specify the number of ping packets the DHCP server sends to an IP address before assigning this address to a requesting client.
Syntax	config dhcp ping_packets <number 0-10>
Description	By default, the DHCP server pings a pool address twice before assigning the address to a DHCP client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client. If the ping is answered, the server will discard the current IP address and try another IP address.
Parameters	<number 0-10> – Specifies the number of ping packets. 0 means there is no ping test.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ping packets:

```
DES-3528:5#config dhcp ping_packets 4
Command: config dhcp ping_packets 4

Success.

DES-3528:5#
```

config dhcp pool ping_timeout

Purpose	Used to specify the amount of time the DHCP server must wait before timing out a ping packet.
Syntax	config dhcp ping_timeout <millisecond 10-2000>
Description	By default, the DHCP server waits 10 milliseconds before timing out a ping packet.
Parameters	<millisecond> – Specifies the amount of time the DHCP server must wait before timing out a ping packet. The default value is 500.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the timeout value for ping packets:

```
DES-3528:5#config dhcp ping_timeout 100
Command: config dhcp ping_timeout 100

Success.

DES-3528:5#
```

create dhcp pool manual_binding

Purpose	Used to specify the distinct identification of the client in dotted-hexadecimal notation or hardware address, for example, 0122.b708.1388, where 01 represents the Ethernet media type and the IP address pair.
Syntax	create dhcp pool manual_binding <pool_name 12> <ipaddr> hardware_address <macaddr> {type [Ethernet IEEE802]}
Description	<p>An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server. The dynamic binding entry will be created when an IP address is assigned to the client from the pool network's address.</p> <p>When creating a DHCP pool manual binding entry if the type is not specified, then the type will be defaulted to ethernet. For the match operation, the hardware type and the hardware address field in the protocol fields will be used to match against the entry.</p> <p>The IP address specified in the manual binding entry must be a range within the network used by the DHCP pool. If the user specifies a conflict IP address, an error message will be returned.</p> <p>If a number of manual binding entries are created, and the network address for the pool is changed so that a conflict occurs, those manual binding entries which are in conflict with the new network address will be automatically deleted.</p>
Parameters	<p><pool name 12> – Specifies the name of the pool.</p> <p><macaddr> – Specifies the hardware address.</p> <p>type – Either Ethernet or IEEE802 can be specified.</p> <p><ipaddr> – Specifies the IP address which will be assigned to the specifies client.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create manual binding entries:

```
DES-3528:5#create dhcp pool manual_binding accounting 10.10.10.1 hardware_address 00-80-C8-02-02-02 type Ethernet
Command: create dhcp pool manual_binding accounting 10.10.10.1 hardware_address 00-80-C8-02-02-02 type Ethernet

Success .

DES-3528:5#
```

delete dhcp pool manual_binding

Purpose	Used to specify the distinct identification of the client in dotted-hexadecimal notation or hardware address to delete.
Syntax	delete dhcp pool manual_binding <pool_name 12> [<ipaddr> all]
Description	An address binding is a mapping between the IP address and MAC address of a client. The delete dhcp pool manual_binding command can be used to delete the manual binding entries.
Parameters	<p><pool name 12> – Specifies the name of the pool.</p> <p><ipaddr> – Specifies the IP address which will be deleted.</p> <p>all – Specifies that all IP addresses will be deleted.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:


To delete manual binding entries:

```
DES-3528:5#delete dhcp pool manual_binding accounting 10.10.10.1
Command: delete dhcp pool manual_binding accounting 10.10.10.1

Success.

DES-3528:5#
```

clear dhcp binding

Purpose	Used to clear all the dynamic binding entries for a pool or all pools.
Syntax	clear dhcp binding [<pool_name 12>[<ipaddr> all] all]
Description	This command clears a specific pool's binding entries, or all binding entries in all pools.
	 NOTE: This command will not clear the dynamic binding entry which matches a manual binding entry.
Parameters	<pool name 12> – Specifies the name of the pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear a dynamic binding entry in pool “accounting”:

```
DES-3528:5#clear dhcp binding all
Command: clear dhcp binding all

Success.

DES-3528:5#
```

show dhcp binding

Purpose	Used to display the current binding entry information.
Syntax	show dhcp binding { <pool_name 12>}
Description	This command displays the current binding entry information.
Parameters	<pool name 12> – Specifies the name of the pool.
Restrictions	None.

Example usage:

To display dynamic binding entries:

```
DES-3528:5#show dhcp binding accounting
Command: show dhcp binding accounting

Pool Name      IP Address      Hardware Address  Type      Status      Lifetime
-----
accounting    192.168.0.1     00-08-C8-08-13-88 Ethernet Manual      86400

Total Entries: 1

DES-3528:5#
```

show dhcp pool manual_binding

Purpose	Used to display the configured manual binding entries.
Syntax	show dhcp pool manual binding {<pool_name 12>}
Description	This command displays the configured manual binding entries.
Parameters	<pool name 12> – Specifies the name of the pool.
Restrictions	None.

Example usage:

To display the configured manual binding entries:

```
DES-3528:5#show dhcp pool manual_binding
Command: show dhcp pool manual_binding

Pool Name      IP Address      Hardware Address  Type
-----
p1             192.168.0.1     00-08-C8-08-13-88 Ethernet
p1             192.168.0.2     00-80-C8-08-13-99 Etherent

Total Entries: 2

DES-3528:5#
```

show dhcp pool

Purpose	Used to display the information for DHCP pool.
Syntax	show dhcp pool { <pool_name 12>}
Description	If the name is not specified, information for all pools will be displayed.
Parameters	<pool name 12> – Specifies the name of the pool.
Restrictions	None.

Example usage:

To display dhcp pool entries:

```
DES-3528:5#show dhcp pool accounting
Command: show dhcp pool accounting

Pool Name      :accounting
Network Address :10.10.10.0/24
Domain Name    :10.10.10.0/24
DNS Server     :10.10.10.1
NetBIOS Name Server :10.10.10.1
NetBIOS Node Type :Hybrid
Default Router :10.10.10.1
Pool Lease     :Infinite
Boot File      :boot.had
Next Server    :192.168.0.1

Total Entries: 1

DES-3528:5#
```


enable dhcp_server

Purpose	Used to enable the DHCP server function.
Syntax	enable dhcp_server
Description	If the DHCP relay is enabled, the DHCP server cannot be enabled. The opposite is also true.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the dhcp_server:

```
DES-3528:5#enable dhcp_server
Command: enable dhcp_server

Success.

DES-3528:5#
```

disable dhcp_server

Purpose	Used to disable the DHCP server function.
Syntax	disable dhcp_server
Description	This command disables the DHCP server function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the dhcp_server:

```
DES-3528:5#disable dhcp_server
Command: disable dhcp_server

Success.

DES-3528:5#
```

show dhcp_server

Purpose	Used to display the status of the DHCP server.
Syntax	show dhcp_server
Description	This command displays the status of the DHCP server.
Parameters	None.
Restrictions	None.

Example usage:

To display the dhcp_server:

```
DES-3528:5#show dhcp_server
```

```
Command: show dhcp_server
```

```
DHCP Server Global State: Disable
Ping Packet Number      : 2
Ping Timeout            : 500 ms
```

```
DES-3528:5#
```

clear dhcp conflict_ip

Purpose	Used to clear an entry or all entries from the conflict IP database.
Syntax	clear dhcp conflict_ip [<ipaddr> all]
Description	This command clears an entry or all entries from the conflict IP database.
Parameters	<ipaddr> – The IP address to be cleared. all – All IP addresses will be cleared.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear an IP address 10.20.3.4 from the conflict database:

```
DES-3528:5#clear dhcp conflict_ip 10.20.3.4
```

```
Command: clear dhcp conflict_ip 10.20.3.4
```

```
Success.
```

```
DES-3528:5#
```

show dhcp conflict_ip

Purpose	Used to display the IP address that has been identified as being in conflict.
Syntax	show dhcp conflict_ip {<ipaddr>}
Description	The DHCP server will use PING packets to determine whether an IP address is in conflict with other hosts before binding it's IP. The IP address which has been identified as in conflict will be moved to the conflict IP database. The system will not attempt to bind the IP address to the conflict IP database unless the user clears it from the conflict IP database.
Parameters	<ipaddr> – The IP address to be displayed.
Restrictions	None.

Example usage:

To display entries in the DHCP conflict IP database:

```
DES-3528:5#show dhcp conflict_ip
```

```
Command: show dhcp conflict_ip
```

```
IP Address           Detection Method      Detection Time
-----
```

```
Total Entries: 0
```

```
DES-3528:5#
```

CABLE DIAGNOSTIC COMMANDS

The Cable Diagnostic commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
cable diagnostic	cable_diag ports [<portlist> all]

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

cable diagnostic

Purpose	Used to diagnose 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. Linked: This pair has been connected to partner network device and the link is up. ShutDown: This pair has been connected to another network device, but the partner is power off. Open: This pair is left open. Short: This pair has been shorted between two lines of its own. CrossTalk: This pair has been shorted between two lines of different pairs. No Cable: There is no pair connected to the port. -: This pair has been connected to another network device normally, but other pair has error. Unknown: The last diagnosis do not obtain the cable' status, please try it again.
Syntax	cable_diag ports [<portlist> all]
Description	When a port is in link up status, the diagnostic will obtain the distance of the cable. Since the status is link-up, the cable will not have any problem. Since this diagnostic is for copper cable, the port with fiber cable will be skipped from the diagnostic. If the link is up, the abnormal results won't be shown and the cable length item indicates the length of the cable. If the link is down the reason may be that its partner has powered off or the port is disabled, the abnormal results won't be shown and the cable length item shows the length of the cable. If the link is down and there is some error in the cable, the abnormal results will be shown, but the cable length item won't be shown.
Parameters	<i>all</i> – Indicate all ports will be displayed. <i><portlist></i> – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To do the cable diagnostic on ports 1-7 on the Switch:

```
DES-3528:5#cable_diag ports 1-7
```

```
Command: cable_diag ports 1-7
```

```
Perform Cable Diagnostics : 1-7
```

Port	Type	Link Status	Test Result	Cable Length (M)
1	FE	Link Down	No Cable	-
2	FE	Link Down	No Cable	-
3	FE	Link Down	No Cable	-
4	FE	Link Down	No Cable	-
5	FE	Link Down	No Cable	-
6	FE	Link Down	No Cable	-
7	FE	Link Down	No Cable	-

```
DES-3528:5#
```

CONNECTIVITY FAULT MANAGEMENT COMMANDS

The Connectivity Fault Management 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 <centiseconds 250 -1000> alarm_reset_time <centiseconds 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 remote_mep	[mepname <string 32> md <string 22> ma <string 22> mepid <int 1-8191> remote_mepid <int 1-8191>]
show cfm fault	{md <string 22> {ma <string 22>}}
show cfm port	<port> {level <int 0-7> direction [inward outward] vlanid <vlanid 1-4094>}
show cfm mipccm	
show cfm pkt_cnt	{[ports <portlist>{rx tx}] rx tx ccm}
clear cfm pkt_cnt	{[ports <portlist>{rx tx}] rx tx ccm}
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>]}
config cfm ccm_fwd	[software hardware]

Command	Parameters
show cfm ccm_fwd	
config cfm mp_ltr_all	[enable disable]
show cfm mp_ltr_all	

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

create cfm md	
Purpose	Used to create a maintenance domain.
Syntax	create cfm md <string 22> level <int 0-7>
Description	Different maintenance domains should have different names.
Parameters	<i>md</i> – Specifies the maintenance domain name. <i>level</i> – Specifies the maintenance domain level.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a cfm maintenance domain.

DES-3528:5# create cfm md op_domain level 2
Command: create cfm md op_domain level 2
Success.
DES-3528:5#

config cfm md	
Purpose	Used to configure parameters of a maintenance domain.
Syntax	config cfm md <string 22> {mip [none auto explicit] sender_id [none chassis manage chassis_manage]} (1)
Description	Creation of MIPs on a MA is useful for tracing the link MIP by MIP. It also allows the user to perform loop-back from MEP to an MIP.
Parameters	<i>md</i> – Specifies the maintenance domain name. <i>mip</i> – Specifies and controls the creation of MIPs. <i>none</i> – Specifies that MIPs will not be created. This is the default value. <i>auto</i> – MIPs can always be created on any ports in this MD, if that port is not configured with a MEP of this MD. For the intermediate switch in a MA, the setting must be auto in order for the MIPs to be created on this device. <i>explicit</i> – MIPs can be created on any ports in this MD, only if the existing lower level has an MEP configured on that port, and that port is not configured with an MEP of this MD. <i>sender_id</i> – Specifies and control the information to be advertised. <i>none</i> – Specifies that there is no information to be advertised. This is the default value. <i>chassis</i> – Advertises the Chassis ID information. <i>manage</i> – Advertises the Management Address information. <i>chassis_manage</i> – Advertises both Management Address and Chassis ID information.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure cfm on a maintenance domain:

```
DES-3528:5#config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DES-3528:5#
```

create cfm ma

Purpose	Used to create a maintenance association.
Syntax	create cfm ma <string 22> md <string 22>
Description	Different MAs in a MD must have different MA Names. Different MAs in different MDs may have the same MA Name.
Parameters	<i>md</i> – Specifies the maintenance domain name. <i>ma</i> – Specifies the maintenance association name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a cfm maintenance association:

```
DES-3528:5#create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DES-3528:5#
```

config cfm ma

Purpose	Used to configure a 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 a MA can be located in different devices. MEPs must be created on ports of these devices explicitly. An 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 the configuration integrity check.
Parameters	<i>md</i> – Specifies the maintenance domain name. <i>ma</i> – Specifies the maintenance association name. <i>vlanid</i> – Specifies the VLAN Identifier. Different MAs must be associated with different VLANs. <i>mip</i> – Specifies the control creation of MIPs. <i>none</i> – No MIPs will be created. <i>auto</i> – MIPs can always be created on any ports in this MA, if that port is not configured with an MEP of that MA. <i>explicit</i> – MIP can be created on any ports in this MA, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MA. <i>defer</i> – Inherit the settings configured for the maintenance domain that this MA is associated with. This is the default value. <i>sender_id</i> – Specifies and control the information to be advertised. <i>none</i> – Specifies that there is no information to be advertised. This is the default value. <i>chassis</i> – Advertises the Chassis ID information.

config cfm ma

manage – Advertises the Management Address information.
chassis_manage – Advertises both Management Address and Chassis ID information.
ccm_interval – Specifies the CCM interval.
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.
mepid_list – Specify the MEPIDs contained in the maintenance association. The range of MEPID is 1-8191.
add – Add MEPID(s).
delete – Specifies to delete MEPID(s).
 By default, there's no MEPID in a newly created maintenance association.

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

Example usage:

To configure cfm maintenance association:

```
DES-3528:5#config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec
Command: config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec

Success.

DES-3528:5#
```

create cfm mep

Purpose Used to create a cfm MEP.

Syntax **create cfm mep** <string 32> mepid <int 1-8191> md <string 22> ma <string 22> direction [inward | outward] port <port>

Description Different MEP in the same MA must have different MEP ID. MD name, MA name, and MEP ID together can identify a MEP.
 Different MEP on the same device must have a different MEP name.
 Before an MEP is created, its MEPID should be configured in MA's MEPID list.

Parameters *mep* – Specifies the MEP name. It's unique among all MEPs configured on the device.
mepid – Specifies the MEP MEPID. It should be configured in MA's MEPID list.
md – Specifies the maintenance domain name.
ma – Specifies the maintenance association name.
direction – Specifies the MEP direction.
inward – Specifies the inward facing (up) MEP.
outware – Specifies the outward facing (down) MEP.
port – Specifies the port number. This port should be a member of the MA's associated VLAN.

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

Example usage:

To create a cfm MEP.

```
DES-3528:5#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-3528:5#
```

config cfm mep

Purpose	Used to configure parameters of a MEP.
Syntax	config cfm mep [<i>mepname</i> <string 32> <i>mepid</i> <int 1-8191> <i>md</i> <string 22> <i>ma</i> <string 22>] { <i>state</i> [<i>enable</i> <i>disable</i>] <i>ccm</i> [<i>enable</i> <i>disable</i>] <i>pdu_priority</i> <int 0-7> <i>fault_alarm</i> [<i>all</i> <i>mac_status</i> <i>remote_ccm</i> <i>error_ccm</i> <i>xcon_ccm</i> <i>none</i>] <i>alarm_time</i> <centiseconds 250 -1000> <i>alarm_reset_time</i> <centiseconds 250-1000>}(1)
Description	An MEP may generate 5 types of Fault Alarms, as shown below by their priorities from high to low: Cross-connect CCM Received: priority 5 Error CCM Received: priority 4 Some Remote MEP Down: priority 3 Some Remote MEP MAC Status Error: priority 2 Some Remote MEP Defect Indication: priority 1 If multiple types of faults occur on a MEP, only the fault of the highest priority will be alarmed.
Parameters	<i>mepname</i> – Specifies the MEP name. It's unique among all MEPs configured on the device. <i>mepid</i> – Specifies the MEP MEPID. It should be configured in MA's MEPID list. <i>md</i> – Specifies the maintenance domain name. <i>ma</i> – Specifies the maintenance association name. <i>state</i> – Specifies the MEP administrative state. <i>enable</i> – MEP is enabled. <i>disable</i> – MEP is disabled. This is the default value. <i>ccm</i> – Specifies the CCM transmission state. <i>enable</i> – CCM transmission enabled. <i>disable</i> – CCM transmission disabled. This is the default value. <i>pdu_priority</i> – Specifies the 802.1p priority to be set in CCMs and LTMs messages transmitted by the MEP. The default value is 7. <i>fault_alarm</i> – Control types of fault alarms sent by the MEP. <i>all</i> – Specifies that all types of fault alarms will be sent. <i>mac_status</i> – Only Fault Alarms whose priority is equal to or higher than "Some Remote MEP MAC Status Error" will be sent. <i>remote_ccm</i> – Only Fault Alarms whose priority is equal to or higher than "Some Remote MEP Down" will be sent. <i>error_ccm</i> – Only Fault Alarms whose priority is equal to or higher than "Error CCM Received" will be sent. <i>xcon_ccm</i> – Only Fault Alarms whose priority is equal to or higher than "Cross-connect CCM Received" will be sent. <i>none</i> – No fault alarm is sent. This is the default value. <i>alarm_time</i> – The time that a defect must last before the fault alarm can be sent. The default value is 2 seconds. <i>alarm_reset_time</i> – The timer must be clear of any alarm defects before the fault can be re-

config cfm mep

alarmed. The default value is 10 seconds

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

Example usage:

To configure the cfm mep:

```
DES-3528:5#config cfm mep mepid 1 md 1 ma 1 state enable ccm enable
```

```
Command: config cfm mep mepid 1 md 1 ma 1 state enable ccm enable
```

Success.

```
DES-3528:5#
```

delete cfm mep

Purpose Used to delete a 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 delete a created MEP.

Parameters

- mepname* – Specifies the MEP name. It's unique among all MEPs configured on the device.
- mepid* – Specifies the MEP MEPID. It should be configured in MA's MEPID list.
- md* – Specifies the maintenance domain name.
- ma* – Specifies the maintenance association name.

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

Example usage:

To delete cfm mep:

```
DES-3528:5#delete cfm mep mepname mep1
```

```
Command: delete cfm mep mepname mep1
```

Success.

```
DES-3528:5#
```

delete cfm ma

Purpose Used to delete a 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

- md* – Specifies the maintenance domain name.
- ma* – Specifies the maintenance association name.

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

Example usage:

To delete a cfm ma:

```
DES-3528:5#delete cfm ma opl md 3
Command: delete cfm ma opl md 3

Success.

DES-3528:5#
```

delete cfm md

Purpose	Used to delete a created maintenance domain.
Syntax	delete cfm md <string 22>
Description	All MEPs and maintenance associations created in the maintenance domain will be deleted automatically.
Parameters	md – Specifies the maintenance domain name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a cfm md:

```
DES-3528:5#delete cfm md 3
Command: delete cfm md 3

Success.

DES-3528:5#
```

enable cfm

Purpose	Used to enable CFM globally.
Syntax	enable cfm
Description	This command is used to enable CFM globally.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable cfm:

```
DES-3528:5#enable cfm
Command: enable cfm

Success.

DES-3528:5#
```

disable cfm

Purpose	Used to disable CFM globally.
Syntax	disable cfm
Description	This command is used to disable CFM globally.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable cfm:

```
DES-3528:5#disable cfm
Command: disable cfm

Success.

DES-3528:5#
```

config cfm ports

Purpose	Used to enable or disable CFM function on per-port basis.
Syntax	config cfm ports <portlist> state [enable disable]
Description	By default, CFM function is disabled on all ports. If CFM is disabled on a port: <ul style="list-style-type: none"> • 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 Loop-back or Linktrace test on those MEPs, it will prompt user that CFM function is disabled on that port.
Parameters	<i>ports</i> – Specifies the logical port list. <i>state</i> – Is used to enable or disable CFM function.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure cfm ports:

```
DES-3528:5#config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

DES-3528:5#
```

show cfm ports

Purpose	Used to show cfm state of specified ports.
Syntax	show cfm ports <portlist>
Description	CFM state of specified ports will be shown.
Parameters	<i>ports</i> – Specifies the logical port list.
Restrictions	None.

Example usage:

To display cfm ports:

```
DES-3528:5#show cfm ports 3-6
Command: show cfm ports 3-6

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

DES-3528:5#
```

show cfm

Purpose	Used to show CFM information.
Syntax	show cfm {[md <string 22> {ma <string 22> {mepid <int 1-8191>}} mepname <string 32>]}
Description	This command is used to show CFM information.
Parameters	<i>md</i> – Specifies the maintenance domain name. <i>ma</i> – Specifies the maintenance domain name. <i>mepid</i> – Specifies the MEP MEPID. <i>mepname</i> – Specifies the MEP name.
Restrictions	None.

Example usage:

To display cfm:

```
DES-3528:5#show cfm
Command: show cfm

CFM State: Enabled

Level  MD Name
-----  -
2       op_domain

DES-3528:5#
```

Example usage:

To display cfm md:

```
DES-3528:5#show cfm md op_domain
Command: show cfm md op_domain

MD Level      : 2
MIP Creation: Explicit
SenderID TLV: None
VID   MA Name
----  -
1     op1

DES-3528:5#
```

Example usage:

To display cfm mepname:

```
DES-3528:5#show cfm mepname mepl
Command: show cfm mepname mepl

Name                : mepl
MEPID               : 1
Port                : 1
Direction           : inward
CFM Port State      : enabled
MAC Address         : XX-XX-XX-XX-XX-XX
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       : None
Next LTM Trans ID   : 27
RX Out-of-Sequence CCMs: 0
RX Cross-connect CCMs : 0
RX Error CCMs       : 0
RX Port Status CCMs : 0
RX If Status CCMs   : 0
RX In-order LBRs    : 0
TX CCMs             : 1234
TX LBMs             : 0

Remote MEP Status
MEPID  MAC Address  Status  RDI  PortSt  IfSt      Detect Time
-----
2      XX-..-XX-XX  OK      Yes  Blocked Up        2009-01-01 12:00:00
3      XX-..-XX-XX  IDLE    No   No       No        2009-01-01 12:00:00
4      XX-..-XX-XX  OK      No   Up       Down      2009-01-01 12:00:00
8      XX-..-XX-XX  START   No   Up       Up        2009-01-01 12:00:00
12     XX-..-XX-XX  FAILED  No   Up       Up        2009-01-01 12:00:00
8      XX-..-XX-XX  OK      No   Up       Up        2009-01-01 12:00:00
DES-3528:5#
```

show cfm fault

Purpose	Used to show fault MEPs.
Syntax	show cfm fault {md <string 22> {ma <string 22>}}
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 fault status by MEPs.
Parameters	<i>md</i> – Specifies the maintenance domain name. <i>ma</i> – Specifies the maintenance domain name.
Restrictions	None.

Example usage:

To display cfm fault:

```
DES-3528:5#show cfm mep fault
Command: show cfm mep fault

MD Name      MA Name      MEPID      Status
-----
op_domain    op1          1          Cross-connect CCM Received

DES-3528:5#
```

show cfm port

Purpose	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 MEPs and MIPs created on a port.
Parameters	<p><i>port</i> – Specifies the port number.</p> <p><i>level</i> – Specifies the MD Level. If not specified, all levels are shown.</p> <p><i>direction</i> – Specifies the MEP direction.</p> <p><i>inward</i> – Inward facing MEP.</p> <p><i>outward</i> – Outward facing MEP.</p> <p>If not specified, both directions and MIPs are shown.</p> <p><i>vlanid</i> – Specifies the VLAN identifier. If not specified, all VLANs are shown.</p>
Restrictions	None.

Example usage:

To display cfm ports:

```
DES-3528:5#show cfm port 1
Command: show cfm port 1

MAC Address: 10:10:90:08:8g:12

MD Name      MA Name      MEPID Level Direction VID
-----
op_domain    op1          1      2      inward  2
cust_domain  cust1        8      4      inward  2
serv_domain  serv2        MIP    3              2

DES-3528:5#
```

show cfm mipccm

Purpose	Used to show MIPCCM database entries.
Syntax	show cfm mipccm
Description	All entries in the MIPCCM database will be shown. The MIPCCM entry is similar to FDB which keeps the forwarding port information for a MAC entry.
Parameters	None.
Restrictions	None.

Example usage:

To display the MIPCCM database entries:

```
DES-3528:5#show cfm mipccm
```

```
Command: show cfm mipccm
```

MA	VID	MAC Address	Port
-----	----	-----	-----
opma	1	00-01-02-03-04-05	2
opma	1	00-01-02-03-04-05	3

```
Total: 2
```

```
DES-3528:5#
```

cfm linktrace

Purpose Used to issue a CFM linktrack 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 linktrack message.

Parameters

- <macaddr>* – Specifies the destination MAC address.
- mepname* – Specifies the MEP name.
- mepid* – Specifies the MEP MEPID.
- md* – Specifies the maintenance domain name.
- ma* – Specifies the maintenance association name.
- ttl* – Specifies the linktrace message TTL value. The default value is 64.
- pdu_priority* – The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA.

Restrictions None.

Example usage:

To create a cfm linktrace:

```
DES-3528:5#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-3528:5#
```

show cfm linktrace

Purpose Used to show linktrace responses.

Syntax `show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {trans_id <uint>}`

Description The maximum linktrace responses a device can hold is 64.

Parameters

- mepname* – Specifies the MEP name.
- mepid* – Specifies the MEP MEPID.
- md* – Specifies the maintenance domain name.
- ma* – Specifies the maintenance association name.
- trans_id* – Specifies the identifier of the transaction to show.

Restrictions None.

Example usage:

To display the cfm linktrace:

```
DES-3528:5#show cfm linktrace mep mep1
Command: show cfm linktrace mep mep1

Trans ID   Source MEP       Destination
-----
26         mep1            00-01-02-03-04-05

DES-3528:5#5#show cfm linktrace mep mep1 trans_id 26
Command: show cfm linktrace mep mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 00-01-02-03-04-05
Start Time 2009-01-01 12:00:00

Hop MEPID  MAC Address      Forwarded  Relay Action
---
-         00-01-02-03-04-05  Yes       FDB
-         00-01-02-03-04-05  Yes       MPDB
8100     00-01-02-03-04-05  No        Hit

DES-3528:5#
```

delete cfm linktrace

Purpose	Used to delete received linktrace responses.
Syntax	<code>delete cfm linktrace {[md <string 22> {ma <string 22> {mepid <int 1-8191>}} mepname <string 32>}}</code>
Description	This command deletes the stored link trace response data that is initiated by the specified MEP.
Parameters	<i>mepname</i> – Specifies the MEP name. <i>mepid</i> – Specifies the MEP MEPID. <i>md</i> – Specifies the maintenance domain name. <i>ma</i> – Specifies the maintenance association name.
Restrictions	None.

Example usage:

To delete a cfm linktrace:

```
DES-3528:5#delete cfm linktrace mep mep1
Command: delete cfm linktrace mep mep1

Success.

DES-3528:5#
```

config cfm ccm_fwd

Purpose	Used to configure CCM PDUs forwarding mode.
Syntax	config cfm ccm_fwd [software hardware]
Description	<p>This command is for test purposes. For ordinary user, it is not suggested to use this command.</p> <p>By default, the CCM message is handled and forwarded by software. The software can handle the packet based on behaviour defined by the standard. Under a strict environment, there may be substantial amount of CCM packets, and it will consume substantial amount of CPU resource. To meet the performance requirement, the handling of CCM can be changed to hardware mode. This function is especially useful for domain's intermediate device since they only have MIPS. Note that this command can only be used under assistance of technical personnel.</p>
Parameters	<p><i>software</i> – Specifies to forward by software.</p> <p><i>hardware</i> – Specifies to forward by hardware.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the cfm ccm forwarding mode:

```
DES-3528:5#config cfm ccm_fwd_mode hardware
Command: config cfm ccm_fwd_mode hardware

Success.

DES-3528:5#
```

cfm loopback

Purpose	Used to show MEPs and MIPs created on a port.
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	The MAC address represents that the destination MEP or MIP which can be reached by this MAC address. The MEP represents the source MEP to initiate the loop-back message. You can press Ctrl+C to exit loop-back test.
Parameters	<p><i><macaddr></i> – Specifies the destination MAC address.</p> <p><i>mepname</i> – Specifies the MEP name.</p> <p><i>mepid</i> – Specifies the MEP MEPID.</p> <p><i>md</i> – Specifies the maintenance domain name.</p> <p><i>ma</i> – Specifies the maintenance association name.</p> <p><i>num</i> – Specifies the number of LBMs to be sent. The default value is 4.</p> <p><i>length</i> – Specifies the payload length of LBM to be sent. The default is 0.</p> <p><i>pattern</i> – Specifies an arbitrary amount of data to be included in a Data TLV, along with an indication of whether the Data TLV is to be included.</p> <p><i>pdu_priority</i> – 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 configure cfm loop-back:

```
DES-3528:5#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-3528:5#
```

show cfm pkt_cnt

Purpose	Used to show CFM packet RX/TX counters.
Syntax	show cfm pkt_cnt {[ports <portlist>{rx tx}] rx tx ccm}
Description	CFM packet counters will be shown.
Parameters	<i>ports</i> – Specifies which ports' counter to show. If not specified, all ports will be shown. <i>{rx tx}</i> – Shows RX or TX packet counter. If none is specified, both of them are shown. <i>ccm</i> - Shows the CCM transmission state.
Restrictions	None.

Example usage:

The following example displays the statistics for CFM packets.

VidDrop: The packets dropped due to invalid VID.

Opcodrop: The packets dropped due to unrecognized CFM opcode.

```
DES-3528:5#show cfm pkt_cnt
```

```
Command: show cfm pkt_cnt
```

CFM RX Statistics

```
-----
```

Port	CCM	LBR	LBM	LTR	LTM	VidDrop	OpcoDrop	Sum
1	0	0	0	0	0	0	0	0
2	254	0	0	0	0	0	0	254
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	3	0	0	0	0	0	3
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
Total	254	3	0	0	0	0	0	257

CFM TX Statistics

```
-----
```

Port	CCM	LBR	LBM	LTR	LTM	Sum
1	0	0	0	0	0	0
2	284	0	0	0	4	292
3	578	0	0	0	0	578
4	578	0	0	0	0	578
5	578	0	0	0	0	578
6	578	0	0	0	0	578

clear cfm pkt_cnt

Purpose	Used to clear the CFM packet RX/TX counters.
Syntax	clear cfm pkt_cnt {[ports <portlist>{rx tx}] rx tx ccm}
Description	This command clears CFM packet counters.
Parameters	<i>ports</i> – Specifies which ports' counter to show. If not specified, all ports will be shown. <i>{rx tx}</i> – Shows RX or TX packet counter. If none is specified, both of them are shown. <i>ccm</i> - Shows the CCM transmission state.
Restrictions	None.

Example usage:

To clear the CFM packet RX/TX counters:

```
DES-3528:5#clear cfm pkt_cnt ports 2 rx
Command: clear cfm pkt_cnt ports 2 rx

Success.

DES-3528:5#
```

config cfm mp_ltr_all

Purpose	Used to configure the CFM mp linktrace on the switch.
Syntax	config cfm mp_ltr_all [enable disable]
Description	This command configures the CFM mp linktrace on the switch.
Parameters	<i>enable</i> – Used to enable the CFM mp linktrace. <i>disable</i> – Used to disable the CFM mp linktrace.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure CFM mp linktrace:

```
DES-3528:5#config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

DES-3528:5#
```

show cfm mp_ltr_all

Purpose	Used to display the CFM mp linktrace settings on the switch.
Syntax	show cfm mp_ltr_all
Description	This command displays the CFM mp linktrace settings on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the CFM mp linktrace on the Switch:

```
DES-3528:5#show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Enabled

DES-3528:5#
```

COMMAND HISTORY LIST

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

Command	Parameters
?	
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 will 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-3528:5#?
..
?
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear fdb
clear log
clear port_security_entry port
clear wac auth_state ports
config 802.1p default_priority
config 802.1p map
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 force_disconnect
config 802.1x fwd_pdu ports
config 802.1x fwd_pdu system
config 802.1x guest_vlan ports
config 802.1x init
```

```
config 802.1x reauth
config access_profile
config account
config accounting service
config address_binding dhcp_snoop max_entry ports
config address_binding ip_mac ipaddress
config address_binding ip_mac ports
config admin local_enable
config arp_aging time
config arprentry
config authen application
config authen parameter attempt
config authen parameter response_timeout
config authen server_group
config authen server_host
config authen_enable
config authen_login
config bandwidth_control
config command_history
config command_prompt
config configuration
config cpu_access_profile profile_id
config dhcp_relay
config dhcp_relay add ipif
config dhcp_relay delete ipif
config dhcp_relay option_82 check
config dhcp_relay option_82 policy
config dhcp_relay option_82 state
config dot1v_protocol_group
config dscp map
config dscp trust
config dst
config fdb aging_time
config filter dhcp_server
config filter extensive_netbios
config filter netbios
config firmware image_id
config flow_meter
config greeting_message
config gvrp timer
config igmp_snooping
config igmp_snooping multicast_vlan
config igmp_snooping multicast_vlan_group
config igmp_snooping querier
config ipif
```

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

To display the parameters for a specific command:

```
DES-3528:5#? config stp
Command: ? config stp

Command: config stp
Usage: {maxage <value 6-40>|maxhops <value 6-40> |hellotime <value 1-2>| forwarddelay <value 4-30>|txholdcount <value 1-10>|fbpdu [enable|disable]|nmi_bpdu_address [dot1d | dot1ad]}
Description: Used to update the STP Global Configuration.
config stp instance_id
config stp mst_config_id
config stp mst_ports
config stp ports
config stp priority
config stp version

DES-3528:5#
```

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	None.

Example usage:

To configure the command history:

```
DES-3528:5#config command_history 20
Command: config command_history 20

Success.

DES-3528:5#
```

show command_history

Purpose	Used to display the command history.
Syntax	show command_history
Description	This command will display the command history.
Parameters	None.
Restrictions	None.

Example usage:

To display the command history:


```
DES-3528:5#show command_history
Command: show command_history

?
? show
show vlan
show command history

DES-3528:5#
```

Appendix A

TECHNICAL SPECIFICATIONS

General	
Standards	IEEE 802.3 NWay auto-negotiation IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1D Spanning Tree IEEE 802.1w Rapid Spanning Tree IEEE 802.1s Multiple Spanning Tree IEEE 802.1Q VLAN IEEE 802.1X Port Based Network Access Control IEEE 802.1p Priority Queues IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3z Gigabit Ethernet. (SFP “Mini GBIC”) IEEE 802.3af standard (only for PoE)
Protocols	CSMA/CD
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
Fiber Optic	1. DEM-310GT (1000BASE-LX) 2. DEM-311GT (1000BASE-SX) 3. DEM-314GT (1000BASE-LHX) 4. DEM-315GT (1000BASE-ZX) 5. DEM-312GT2 (1000BASE-SX) 6. DEM-210 (Single Mode 100BASE-FX) 7. DEM-211 (Multi Mode 100BASE-FX) WDM transceiver Supported: 1. DEM-330T (TX-1550/RX-1310nm), up to 10km, Single-Mode 2. DEM-330R (TX-1310/RX-1550 nm), up to 10km, Single-Mode 3. DEM-331T (TX-1550/RX-1310 nm), up to 40km, Single-Mode 4. DEM-331R (TX-1310/RX-1550 nm), up to 40km, Single-Mode
Topology	Star
Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)

Physical and Environmental	
Internal Power Supply	<p>DES-3528</p> <p>Input: 100~240V, AC/0.5A(Max), 50~60Hz Output: 12V, 1.2A (Max) Internal universal power supply</p> <p>DES-3552</p> <p>Input: 100~240V, AC/0.8A(Max), 50~60Hz Output: 12V, 2.1A (Max) Internal universal power supply</p> <p>DES-3528P</p> <p>Input: 100~240V, AC/6.3A(Max), 50~60Hz Output: 50V, 7.5A(Max), 12V, 1.4A(Max) Internal universal power supply</p> <p>DES-3528DC</p> <p>DC Power Input: 36-75V,DC/ 0.6A (Max) Output: 12V, 1.2A (Max) Internal universal power supply.</p> <p>DES-3528/DES-3552</p> <p>Provides one connector on the rear panel to install an optional external RPS (DPS-200) to enhance the reliability. When the internal power fails, the optional external RPS will take over all the power immediately and automatically.</p> <p>DES-3528P</p> <p>Provides one connector on the rear panel to install an optional external RPS (DPS-600) to enhance the reliability. When the internal power fails, the optional external RPS will take over all the power immediately and automatically.</p>
Power Consumption	<p>DES-3528 - Max. 20.5 watts DES-3528DC - Max 18.38 watts DES-3552 - Max 33.1 watts DES-3528P - Max. 505.1 watts</p>
Operating Temperature	0 - 45°C
Storage Temperature	-40 - 70°C
Operation Relative Humidity	5 – 95% non-condensing
Storage Relative Humidity	5 - 95% non-condensing
Dimensions	<p>DES-3528/DES-3528DC - 441(W) x 210(D) x 44(H) mm DES-3552/DES-3528P - 441(W) x 310(D) x 44(H) mm</p>
Weight	DES-3528 – 2.51kg (5.53lbs)

Physical and Environmental	
	DES-3528DC – 2.52kg (5.55lbs) DES-3552 – 4.09kg (9.01lbs) DES-3528P – 5.42kg (11.94lbs)
EMI	CE Class A, FCC Class A, C-Tick, VCCI Class A
Safety	CB Report, UL

Performance	
Transmission Method	Store-and-forward
Packet Buffer	1 MB per device
Packet Filtering / Forwarding Rate	14,881 pps (10M port) 148,810 pps (100M port) 1,488,100 pps (1 Gbps port)
MAC Address Learning	Automatic update. Supports 16K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.

Appendix B

MITIGATING ARP SPOOFING ATTACKS VIA PACKET CONTENT ACL

Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address (MAC address) when only its IP address is known. This protocol is vulnerable because it can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce ARP protocol, ARP spoofing attacks, and the counter measure brought by D-Link's switches to counter the ARP spoofing attack.

• How Address Resolution Protocol works

In the process of ARP, PC A will, firstly, issue an ARP request to query PC B's MAC address. The network structure is shown in Figure-1.

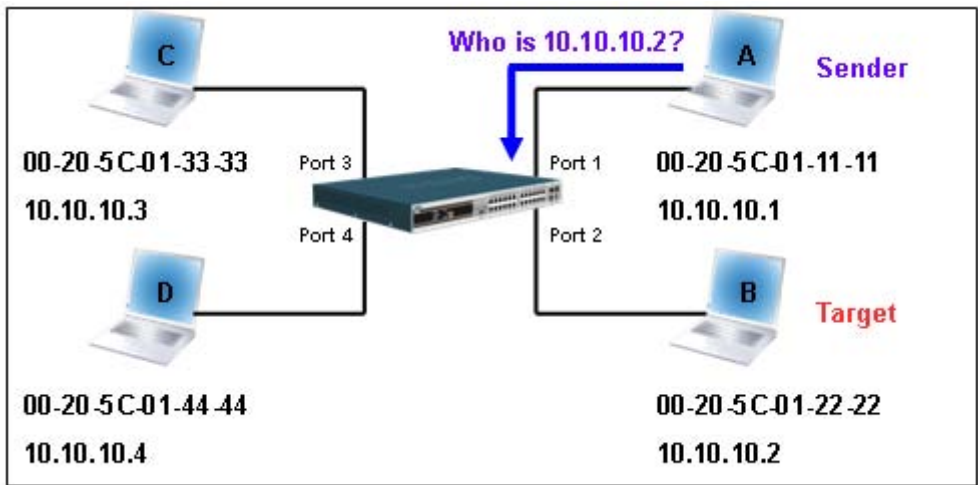


Figure – 1

In the mean time, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00" while PC B's IP address will be written into the "Target Protocol Address", shown in Table-1.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP request	00-20-5C-01-11-11	<u>10.10.10.1</u>	<u>00-00-00-00-00-00</u>	<u>10.10.10.2</u>

Table – 1 (ARP Payload)

The ARP request will be encapsulated into Ethernet frame and sent out. As can be seen in Table-2, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since an ARP request is sent via a broadcast, the "Destination address" is in the format of an Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Destination address	Source address	Ether-type	ARP	FCS
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11			

Table – 2 (Ethernet frame format)

When the switch receives the frame, it will check the “Source Address” in the Ethernet frame’s header. If the address is not in its Forwarding Table, the switch will learn PC A’s MAC and the associated port into its Forwarding Table.



In addition, when the switch receives the broadcast ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure -2).

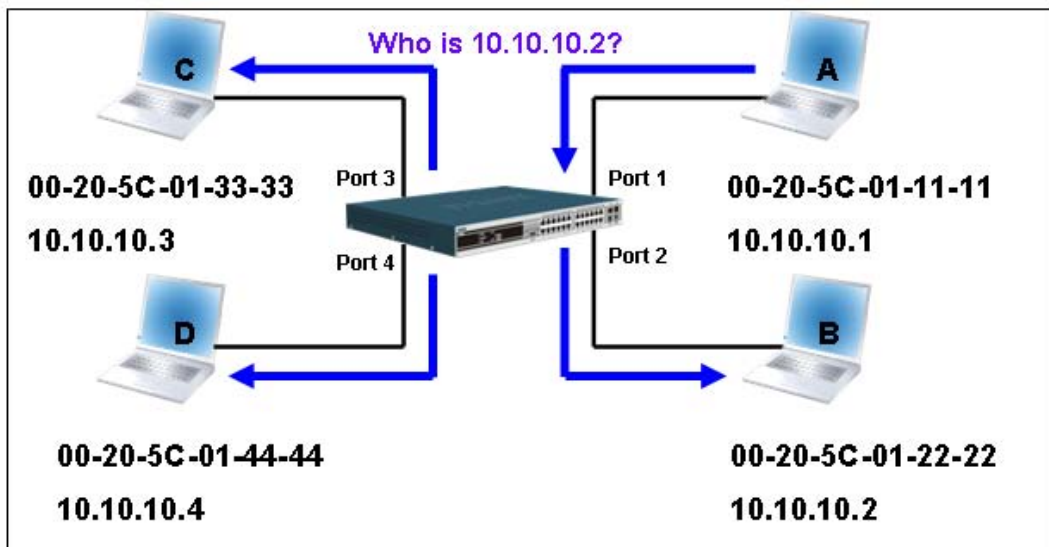


Figure – 2

When the switch floods the frame of ARP requests to the network, all PCs will receive and examine the frame but only PC B will reply to the query as the destination IP address of PC B matches (see Figure-3).

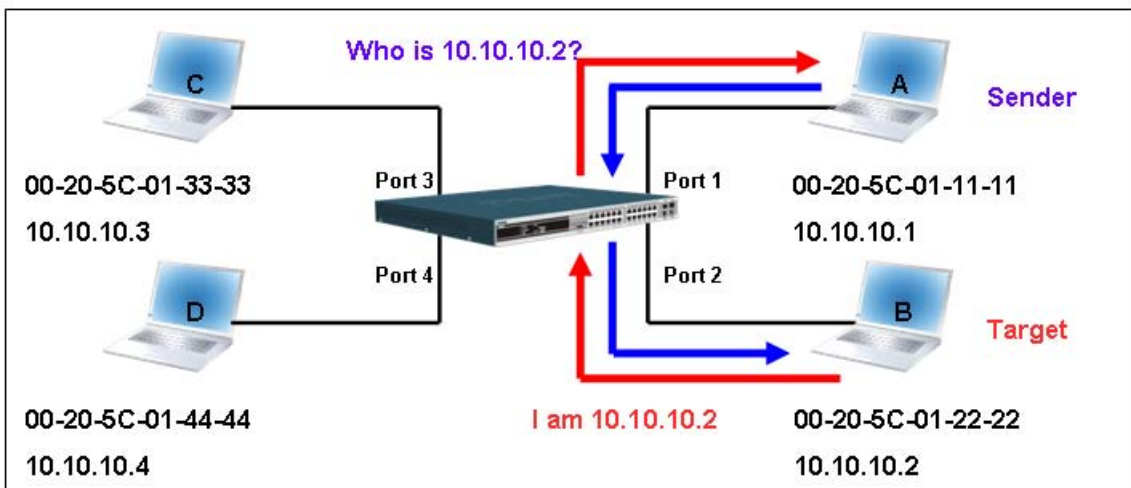


Figure – 3

When PC B replies to the ARP request, its MAC address will be written into “Target H/W Address” in the ARP payload shown in Table-3. The ARP reply will be then encapsulated into the Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP reply	<u>00-20-5C-01-11-11</u>	<u>10.10.10.1</u>	<u>00-20-5C-01-22-22</u>	<u>10.10.10.2</u>

Table – 3 (ARP Payload)

When PC B replies the query, the “Destination Address” in the Ethernet frame will be changed to PC A’s MAC address. The “Source Address” will be changed to PC B’s MAC address (see Table-4).

Destination address	Source address	Ether-type	ARP	FCS
<u>00-20-5C-01-11-11</u>	<u>00-20-5C-01-22-22</u>			

Table – 4 (Ethernet frame format)

The switch will also examine the “Source Address” of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B’s MAC and update its Forwarding Table.

Forwarding Table

Port1 00-20-5C-01-11-11
 Port2 00-20-5C-01-22-22

• **How ARP spoofing attacks a network**

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service - DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

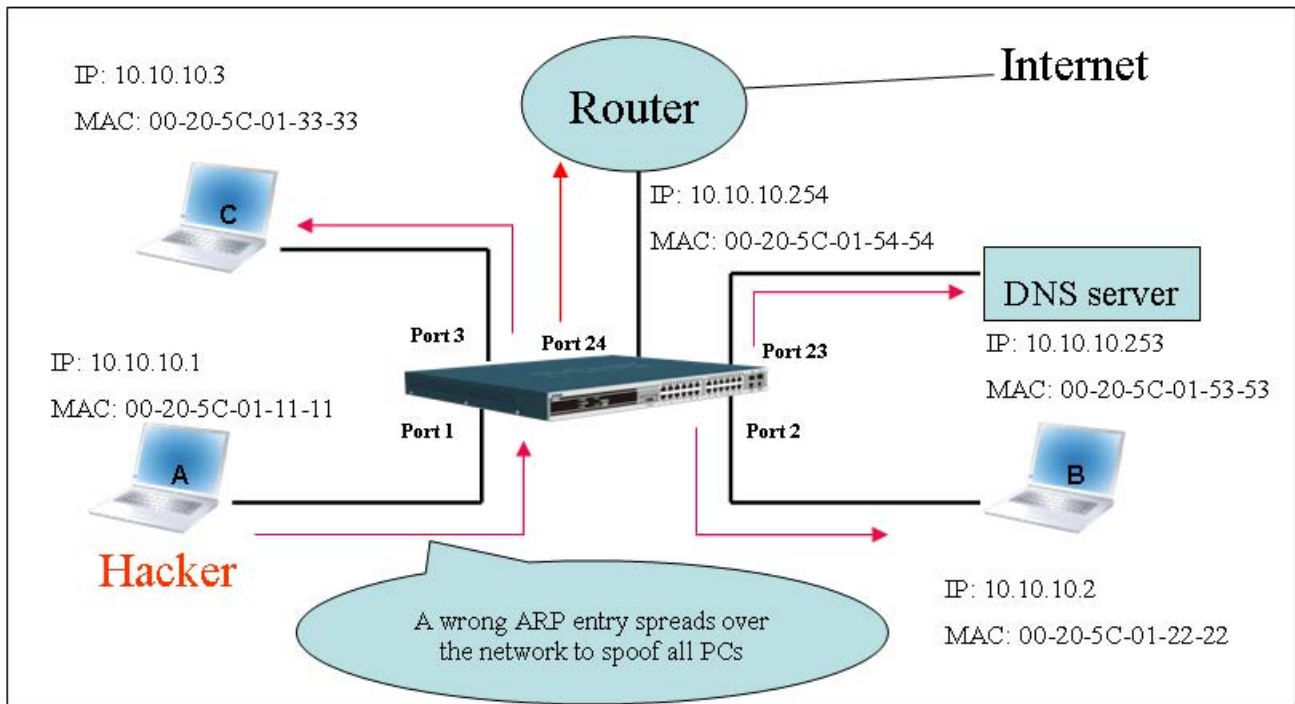


Figure – 4

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of Gratuitous ARP is shown in Table-5.

Ethernet Header			Gratuitous ARP									
Destination address	Source address	Ethernet type	H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address	
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)	
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	806					ARP reply	<u>00-20-5C-01-11-11</u>	<u>10.10.10.254</u>	<u>00-20-5C-01-11-11</u>	<u>10.10.10.254</u>	

Table – 5

A common DoS attack today can be done by associating a nonexistent or specified MAC address to the IP address of the network’s default gateway. The malicious attacker only needs to broadcast ONE Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker cheats the victim’s PC to think that it is a router and cheats the router to think it is the victim. As can be seen in Figure-5 all traffic will be then sniffed by the hacker but the users will not notice anything happening.

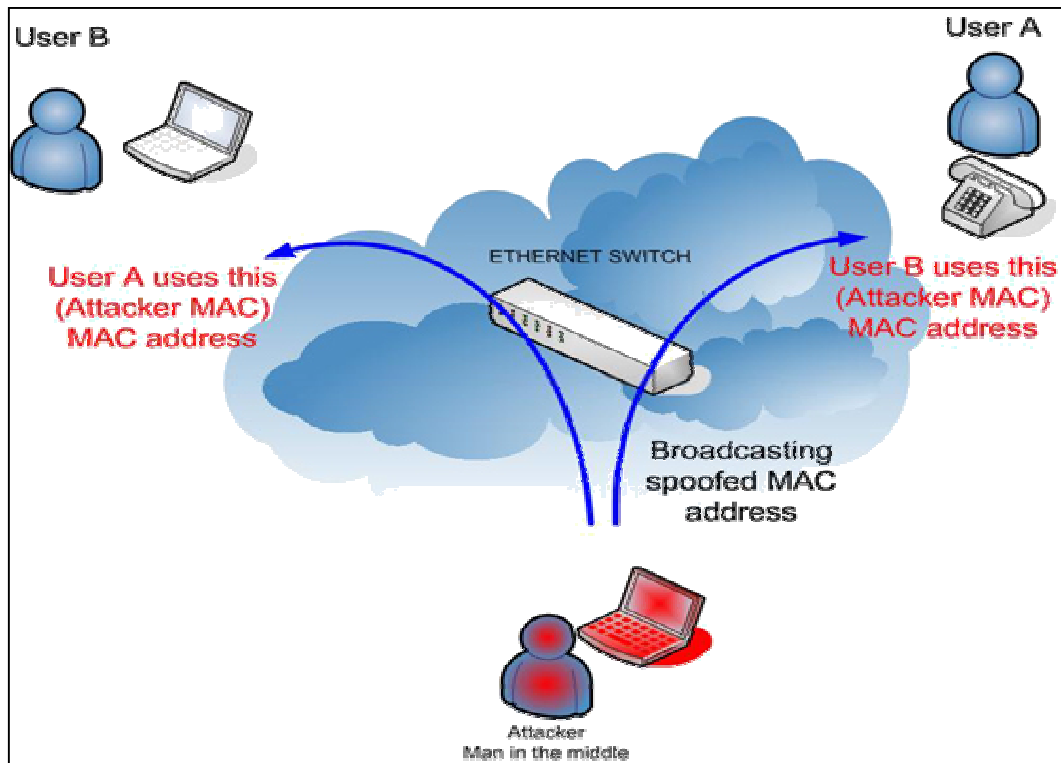
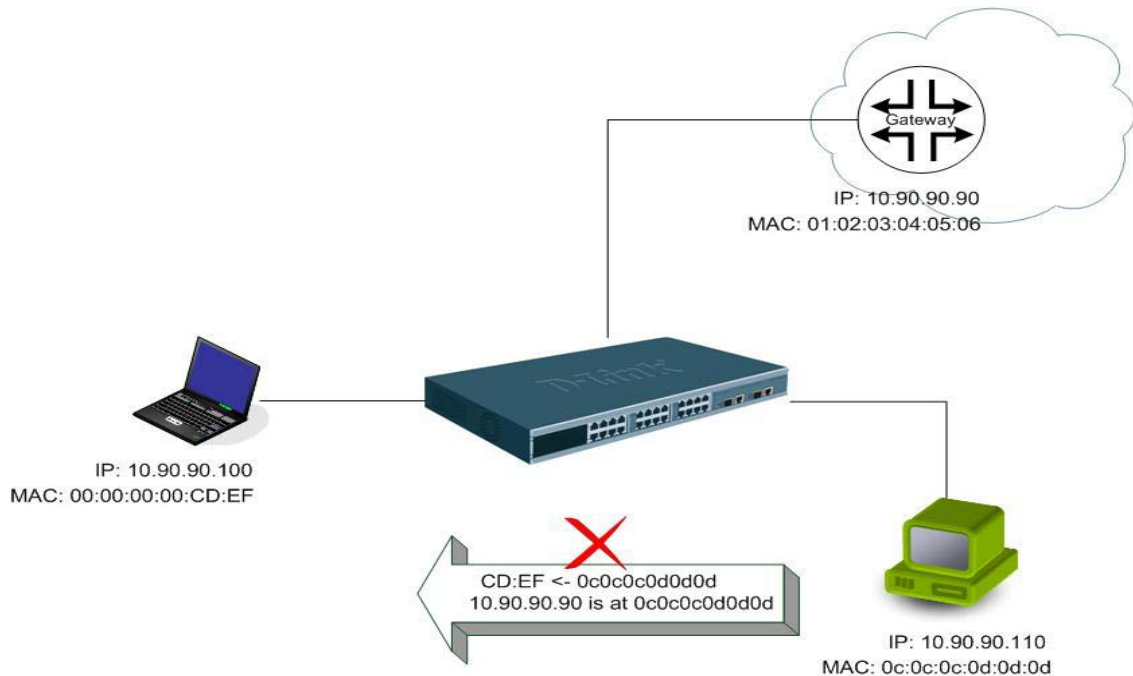


Figure – 5

• Prevent ARP spoofing via packet content ACL

Concerning the common DoS attack today caused by the ARP spoofing, D-Link managed switch can effectively mitigate it via its unique Packet Content ACL.

For that reason the basic ACL can only filter ARP packets based on packet type, VLAN ID, Source and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here using Packet Content ACL on DES-3528 to block the invalid ARP packets which contain fake gateway's MAC and IP binding.



Example topology

Configuration:

The configuration logic is listed below:

1. Only when the ARP matches the Source MAC address in Ethernet, the Sender MAC address and Sender IP address in the ARP protocol can pass through the switch. (In this example, it is the gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL on DES-3528 series enables users to inspect any offset_chunk. An offset_chunk is a 4-byte block in a HEX format which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of 4 offset_chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset_chunks can be applied to each profile and a switch. Therefore, careful consideration is needed for planning the configuration of the valuable offset_chunks.

In Table-6, you will notice that the Offset_Chunk0 starts from 127th and ends at the 2nd byte. It can also be found that the offset_chunk is scratched from 1 but not zero.

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30	Offset Chunk31
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

Table-6: Chunk and Packet offset indicates a completed ARP packet contained in the Ethernet frame, which is the pattern for the calculation of packet offset.

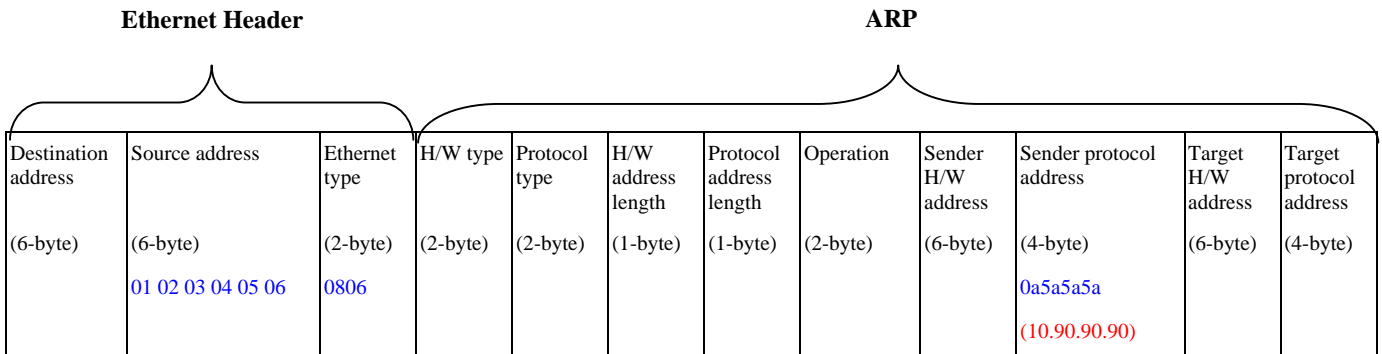


Table – 7: A completed ARP packet contained in Ethernet frame



	Command	Description
Step1	create access_profile profile_id 1 profile_name 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	- Create access profile 1 To match Ethernet Type and Source MAC address.
Step2	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-27 permit	- Configure access profile 1 - Only if the gateway's ARP packet that contains the correct Source MAC in the Ethernet frame can pass through the switch.
Step3	create access_profile profile_id 2 profile_name 2 packet_content_mask offset_chunk_1 3 0x0000FFFF Ethernet Type (2-byte) offset_chunk_2 7 0x0000FFFF SrcIP (First 2-byte) offset_chunk_3 8 0xFFFF0000 SrcIP (Last 2-byte)	- Create access profile 2 - The first Chunk starts from Chunk 3: mask for Ethernet Type (Blue in Table-6: 13 th & 14 th bytes) - The second Chunk starts from Chunk 7: mask for Sender IP (First 2-byte) in ARP packet (Green in Table-6: 29 th & 30 th bytes) - The third Chunk starts from Chunk 8: mask for Sender IP (Last 2-byte) in ARP packet (Brown in Table-6: 31 st & 32 nd bytes)
Step4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 Ethernet Type (2-byte):ARP offset_chunk_2 0x00000A5A SrcIP (First 2-byte): 10.90 offset_chunk_3 0x5A5A0000 SrcIP (Last 2-byte): 90.90 port 1-27 deny	- Configure access profile 2 - The rest of the ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step5	Save	- Save config

Appendix C

PASSWORD RECOVERY PROCEDURE

This section 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:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the switch. After the runtime image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode”. Once the Switch enters the “Password Recovery Mode”, all ports on the Switch will be disabled.

```

Boot ProcedureV1.00.B06
-----
Power On Self Test ..... 100%

MAC Address   : 00-19-5B-EC-32-15
H/W Version   : A1

Please wait, loading V2.00.B33 Runtime image..... 100 %
    
```

```

Password Recovery Mode
>
    
```

3. In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
reset config	The reset config command resets the whole configuration 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.