D-Link®
Building Networks for People

CLI Reference Manual

Product Model : DES-3028/DES-3028P/DES-3028G/DES-3052/DES-3052P

Managed 10/100Mbps Fast Ethernet Switch

Release 2

January 2009 P/N 651ES3028025G

Table of Contents

1

INTRODUCTION

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

This manual provides a reference for all of the commands contained in the CLI. Configuration and management of the Switch via the Web-based management agent is discussed in the Manual. This manual provides a reference for all of the commands contained in the CLI for members of this series, including the DES-3028, DES-3028P, DES-3028G, DES-3052, and DES-3052P. Examples present in this manual may refer to any member of this series and may show different port counts, but are universal to this series of switches, unless otherwise stated. Configuration and management of the Switch via the Web-based management agent is discussed in the User's Guide.

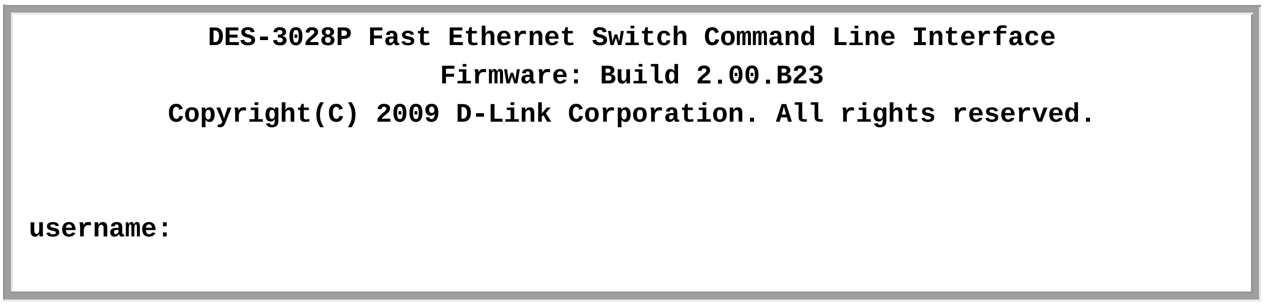
Accessing the Switch via the Serial Port

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

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

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

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-3028P Fast Ethernet Switch Command Line Interface
                       Firmware: Build 2.00.B23
       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-3028P:4#**. This is the command line where all commands are input.

Setting the Switch's IP Address

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

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

```
Boot Procedure                                                V1.00.06
---------------------------------------------------------------------------
Power On Self Test.................................100%
MAC Address : 00-21-91-98-60-77
H/W Version : A1
Please wait, loading V2.00.B23 Runtime image........100%
```

Figure 1-2. Boot screen

The Switch's MAC address can also be found in the Web management program on the **Switch Information (Basic Settings)** window 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-3028P:4#config ipif System ipaddress 10.73.21.11/255.0.0.0
Command: config ipif System ipaddress 10.73.21.11/8
Success.

DES-3028P:4#
```

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.90.90.91 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.

2

USING THE CONSOLE CLI

The DES-3028/28P/28G/52/52P support 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**
- **9600 baud**
- **8 data bits**
- **No parity**
- **One stop bit**
- **No flow control**

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

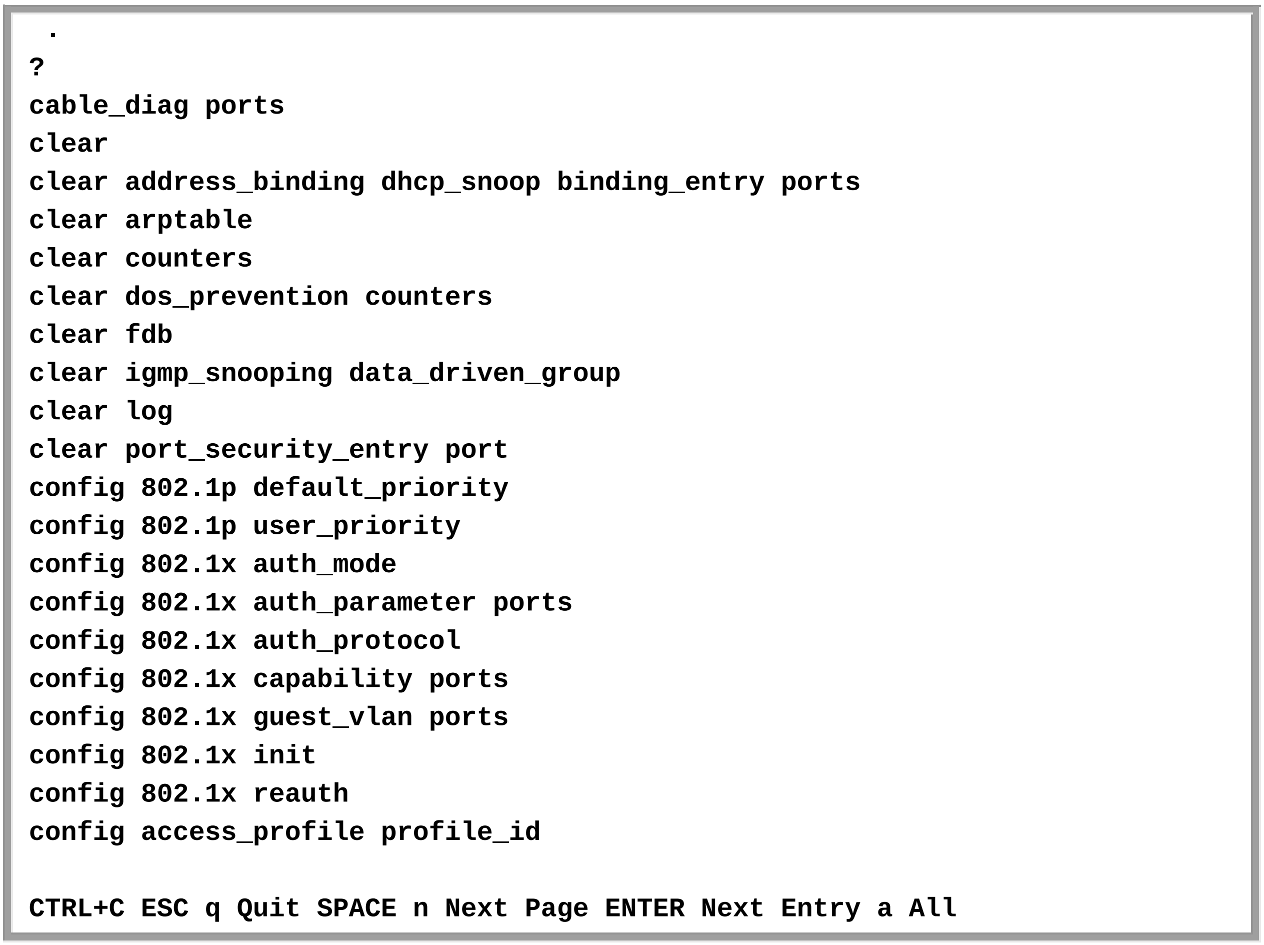
After the Switch reboots and users have logged in, the console looks like this:

```
DES-3028P Fast Ethernet Switch Command Line Interface
Firmware: Build 2.00.B23
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-3028P:4#**.

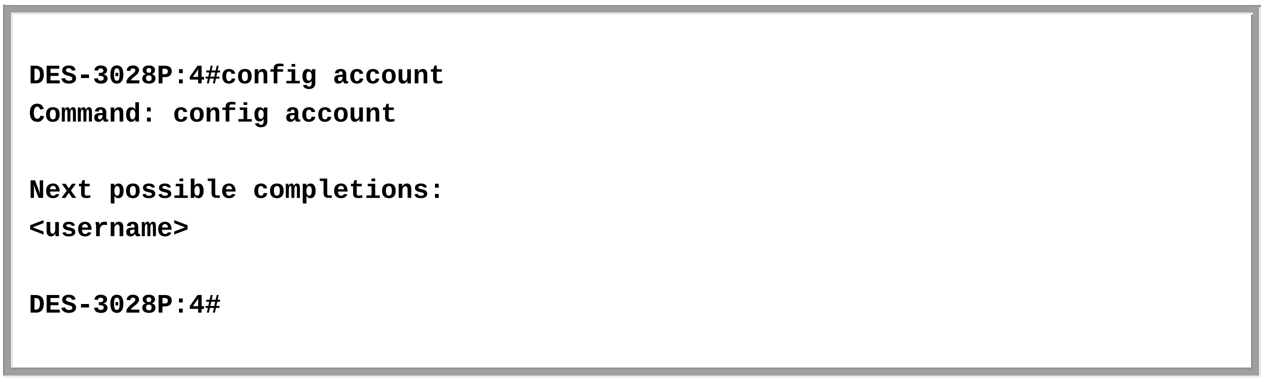
There are a number of helpful features included in the CLI. Entering the **?** command will display a list of all of the top-level commands.



```
 .
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear dos_prevention counters
clear fdb
clear igmp_snooping data_driven_group
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id

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

Figure 2-2. The ? Command

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



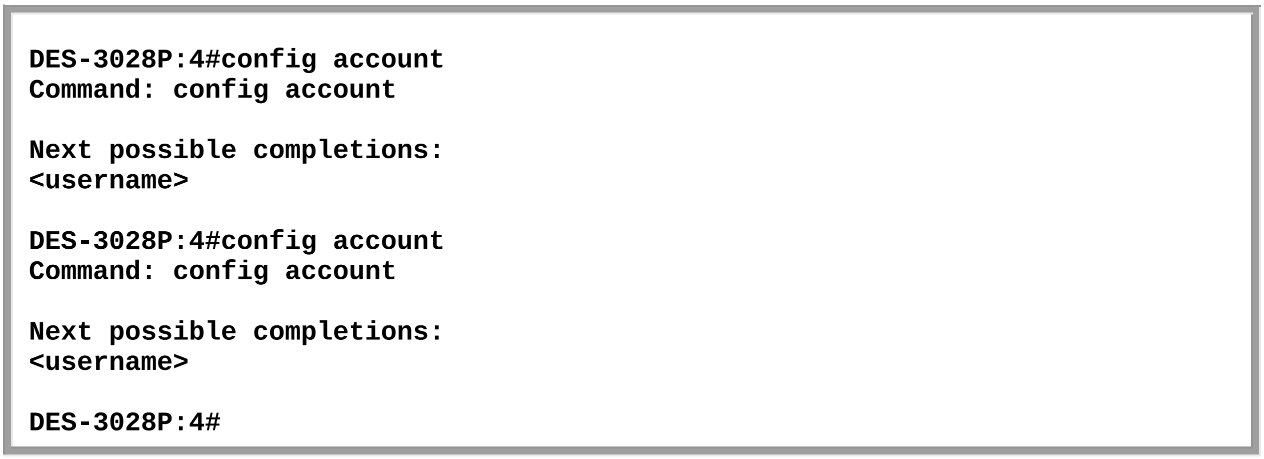
```
DES-3028P:4#config account
Command: config account

Next possible completions:
<username>

DES-3028P:4#
```

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.



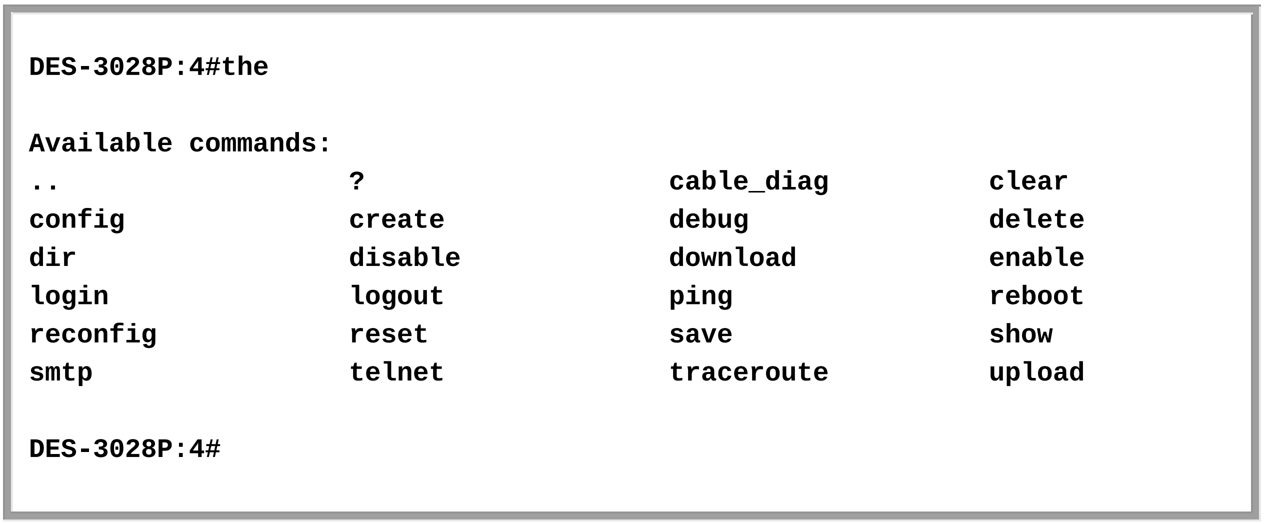
```
DES-3028P:4#config account
Command: config account

Next possible completions:
<username>

DES-3028P:4#config account
Command: config account

Next possible completions:
<username>

DES-3028P:4#
```

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

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

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

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

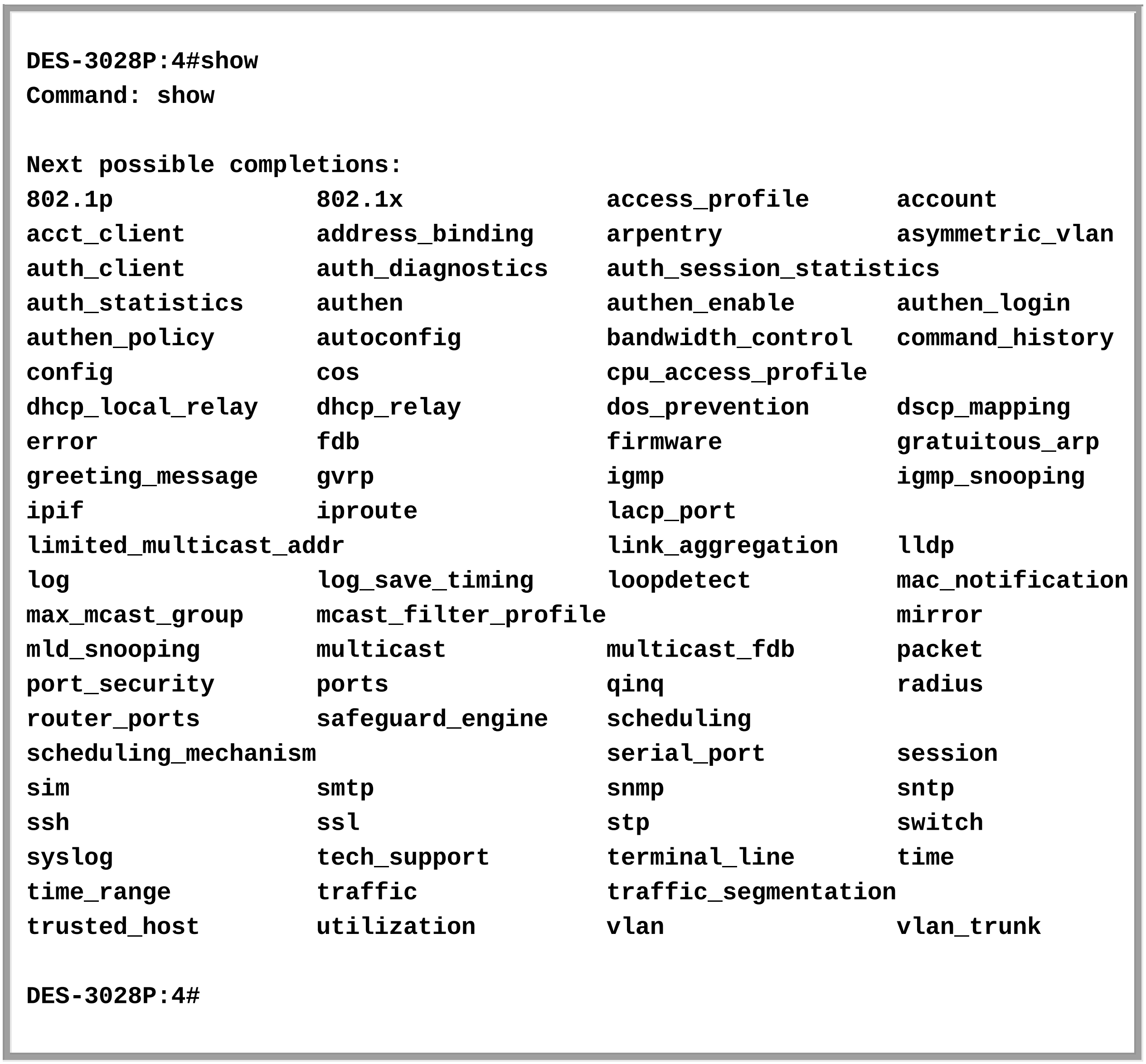


```
DES-3028P:4#the

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

DES-3028P:4#
```

Figure 2-5. The Next Available Commands Prompt

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

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



```
DES-3028P:4#show
Command: show

Next possible completions:
802.1p              802.1x              access_profile      account
acct_client         address_binding     arpentry            asymmetric_vlan
auth_client         auth_diagnostics    auth_session_statistics
auth_statistics     authen              authen_enable       authen_login
authen_policy       autoconfig          bandwidth_control   command_history
config              cos                 cpu_access_profile
dhcp_local_relay    dhcp_relay          dos_prevention      dscp_mapping
error               fdb                 firmware            gratuitous_arp
greeting_message    gvrp                igmp                igmp_snooping
ipif                iproute             lacp_port
limited_multicast_addr                  link_aggregation    lldp
log                 log_save_timing     loopdetect          mac_notification
max_mcast_group     mcast_filter_profile                    mirror
mld_snooping        multicast           multicast_fdb       packet
port_security       ports               qinq                radius
router_ports        safeguard_engine    scheduling
scheduling_mechanism                    serial_port         session
sim                 smtp                snmp                sntp
ssh                 ssl                 stp                 switch
syslog              tech_support        terminal_line       time
time_range          traffic             traffic_segmentation
trusted_host        utilization         vlan                vlan_trunk

DES-3028P:4#
```

Figure 2-6. Next possible completions: Show Command

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

3

COMMAND SYNTAX

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

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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**config ipif <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 | 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 Darren**

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

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	**reset {[config | system]}**
Description	In the above syntax example, users have the option to specify **config** or **system**. It is not necessary to specify either optional value,

{braces}	
	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.
Example command	**reset config**

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

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

4

BASIC SWITCH COMMANDS

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

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

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

enable password encryption

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

Example usage:

To enable password encryption on the Switch.

```
DES-3028P:4#enable password encryption
Command: enable password encryption

Success.

DES-3028P:4#
```

disable password encryption

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

Example usage:

To disable password encryption on the Switch.

```
DES-3028P:4#disable password encryption
Command: disable password encryption

Success.

DES-3028P:4#
```

create account	
Purpose	Used to create user accounts.
Syntax	**create [admin | user] <username 15>**
Description	The **create account** 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 <username>* *user <username>*
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-3028P:4#create account admin dlink
Command: create account admin dlink

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

Success.

DES-3028P:4#
```

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

config account	
Purpose	Used to configure user accounts
Syntax	**config account <username>**
Description	The **config account** command configures a user account that has been created using the **create account** command.
Parameters	*<username>*
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-3028P:4#config account dlink
Command: config account dlink

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

Success.

DES-3028P:4#
```

show account

Purpose	Used to display user accounts.
Syntax	**show account**
Description	Displays 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-3028P:4#show account
Command: show account

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

Total Entries: 1

DES-3028P:4#
```

delete account

Purpose	Used to delete an existing user account.
Syntax	**delete account <username>**
Description	The **delete account** command deletes a user account that has been created using the **create account** command.
Parameters	*<username>*
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account “System”:

```
DES-3028P:4#delete account System
Command: delete account System

Success.

DES-3028P:4#
```

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-3028P:4#show session
Command: show session

ID   Login Time              Live Time     From          Level     Name
--  --------------------    -----------  -----------    -----     -----------
8   00000 days 00:00:37     0:3:36:27    Serial Port    4         Anonymous

Total Entries: 1

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

show switch

Purpose	Used to display general information about the Switch.
Syntax	**show switch**
Description	This command displays information about the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the Switch’s information:

```
DES-3028P:4#show switch
Command: show switch

Device Type         : DES-3028P Fast Ethernet Switch
MAC Address         : 00-19-5B-EF-78-B5
IP Address          : 10.73.21.11 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version   : Build 1.00.B06
Firmware Version    : Build 2.00.B23
Hardware Version    : A1
System Name         :
System Location     :
System Contact      :
Spanning Tree       : Disabled
GVRP                : Disabled
IGMP Snooping       : Disabled
VLAN trunk          : Disabled
802.1x              : Disabled
TELNET              : Enabled(TCP  23)
WEB                 : Enabled(TCP  80)
RMON                : Disabled
SSH                 : Disabled
SSL                 : Disabled
```

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

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-3028P:4#show serial_port
Command: show serial_port

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

DES-3028P:4#
```

config serial_port

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

Example usage:

To configure the baud rate:

```
DES-3028P:4#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200
```

```
Success.

DES-3028P:4#
```

enable clipaging

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

Example usage:

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

```
DES-3028P:4#enable clipaging
Command: enable clipaging

Success.

DES-3028P:4#
```

disable clipaging

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

Example usage:

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

```
DES-3028P:4#disable clipaging
Command: disable clipaging

Success.

DES-3028P:4#
```

enable telnet

Purpose	Used to enable communication with and management of the Switch using the Telnet protocol.

enable telnet	
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-level users can issue this command.

Example usage:

To enable Telnet and configure port number:

```
DES-3028P:4#enable telnet 23
Command: enable telnet 23

Success.

DES-3028P:4#
```

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

Example usage:

To disable the Telnet protocol on the Switch:

```
DES-3028P:4#disable telnet
Command: disable telnet

Success.

DES-3028P:4#
```

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

Example usage:

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

```
DES-3028P:4#telnet 10.53.13.99 tcp_port 23
Command: telnet 10.53.13.99 tcp_port 23
```

enable web

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

Example usage:

To enable HTTP and configure port number:

```
DES-3028P:4#enable web 80
Command: enable web 80

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

DES-3028P:4#
```

disable web

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

Example usage:

To disable HTTP:

```
DES-3028P:4#disable web
Command: disable web

Success.

DES-3028P:4#
```

save

Purpose	Used to save changes in the Switch’s configuration to non-volatile RAM.

save

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

Example usage:

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

```
DES-3028P:4#save
Command: save

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

Success.

DES-3028P:4#
```

reboot

Purpose	Used to restart the Switch.
Syntax	**reboot**
Description	This command is used to restart the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To restart the Switch:

```
DES-3028P:4#reboot
Command: reboot
Are users sure want to proceed with the system reboot? (y|n)
Please wait, the switch is rebooting...
```

reboot force_agree

Purpose	Used to force the Switch to restart.
Syntax	**reboot force_agree**
Description	This command is used to force the Switch to restart.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To force the Switch to restart:

```
DES-3028P:4#reboot force_agree
Command: reboot force_agree

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

reset

Purpose	Used to reset the Switch to the factory default settings.
Syntax	**reset {[config | system]} {force_agree}**
Description	This command is used to restore the Switch's configuration to the default settings assigned from the factory.
Parameters	*config* – If the keyword 'config' is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, and the switch history log. The Switch will not save or reboot. *system* – If the keyword 'system' is specified all of the factory default settings are restored on the Switch. The Switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base. *force_agree* – When force_agree is specified, the reset command will be executed immediately without further confirmation. 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.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#reset config
Command: reset config

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

Success.

DES-3028P:4#
```

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-3028P:4#login
Command: login

UserName:
```

logout

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

Example usage:

To terminate the current user’s console session:

```
DES-3028P:4#logout
```

5

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	
enable greeting_message	
disable 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	Administrator level users can use this command to change the command prompt.
Parameters	*string 16* – The command prompt can be changed by entering a new name of no more that 16 characters. *username* – The command prompt will be changed to the login username. *default* – The command prompt will reset to factory default command prompt.
Restrictions	Only Administrator-level users can issue this command. Other restrictions include: • If the "**reset/reset config**" command is executed, the modified command prompt will remain modified. However, the "**reset system**" command will reset the command prompt to the original factory banner.

Example usage

To modify the command prompt to "AtYourService":

```
DES-3028P:4#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:4#
```

config greeting _message

Purpose	Used to configure the login banner (greeting message).
Syntax	**config greeting _message {default}**
Description	Users can use this command to modify the login banner (greeting

config greeting _message

	message).
Parameters	*default* – If the user enters *default* to the modify banner command, then the banner will be reset to the original factory banner. To open the Banner Editor, click **Enter** after typing the **config greeting_message** command. Type the information to be displayed on the banner by using the commands described on the Banner Editor: 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	Only Administrator-level users can issue this command. Other restrictions include: • If the "**reset/reset config**" command is executed, the modified banner will remain modified. However, the "**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 to read "Say goodnight, Gracie":

```
DES-3028P:4# config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================
                         DGS-3028P Fast Ethernet Switch
                             Command Line Interface

                            Firmware: Build 2.00.B.23
           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-3028P:4#show greeting_message
Command: show greeting_message

=========================================================================
                      DES-3028P Fast Ethernet Switch
                          Command Line Interface

                         Firmware: Build 2.00.B23
        Copyright(C) 2009 D-Link Corporation. All rights reserved.
=========================================================================

DES-3028P:4#
```

6

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 32> | clear_description] mdix [auto|normal|cross]}
show ports	[<portlist>] {description | err_disabled}

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

config ports	
Purpose	Used to configure the Switch’s Ethernet port settings.
Syntax	**[<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | [description <desc 32> | clear_description] mdix [auto|normal|cross]}**
Description	This command allows for the configuration of the Switch’s Ethernet ports. Only the ports listed in the *<portlist>* will be affected.
Parameters	*all* – Configure all ports on the Switch. *<portlist>* – Specifies a port or range of ports to be configured. *medium_type [fiber | copper]* – This applies only to the Combo ports. If configuring the Combo ports this defines the type of medium being configured. *speed* – Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following: • *auto* – Enables auto-negotiation for the specified range of ports. • *[10 | 100 | 1000]* – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 but can be set to slower speeds. • *[half | full]* – Configures the specified range of ports as either full-duplex or half-duplex. • *[master | slave]* – The master setting (1000M/Full_M) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (1000M/Full_S) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for 1000M/Full_M, the other side of the connection must be set for 1000M/Full_S. Any other configuration will result in a link down status for both ports. *flow_control [enable | disable]* – Enable or disable flow control for the specified ports. *learning [enable | disable]* – Enables or disables the MAC address learning on the specified range of ports. *state [enable | disable]* – Enables or disables the specified range of ports. *description <desc 32>* – Enter an alphanumeric string of no more than 32 characters to describe a selected port interface. *clear_description* – Enter this command to clear the port description of the selected port(s). *mdix* – Specifies the MDIX setting of the port. The MDIX setting can be auto, normal or cross. If set to normal state, the port in MDIX mode, can be connected to PC NIC using a straight cable. If set to cross state, the port in mdi mode, can be connected to a port (in mdix mode) on another switch through a straight cable.

config ports

Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#config ports 1-3 speed 10_full state enable
Command: config ports 1-3 speed 10_full state enable

Success.

DES-3028P:4#
```

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	**show ports [<portlist>] {description | err_disabled}**
Description	The show ports command displays the current configurations of a range of ports. No parameters will show all 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.
Restrictions	None.

Example usage:

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

```
DES-3028P:4#show ports
Command show ports

Port   State/         Settings             Connection          Address
        MDI       Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl    Learning
 -----  --------  ---------------------  ---------------------    --------
 1      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 2      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 3      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 4      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 5      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 6      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 7      Enabled   Auto/Disabled          100M/Full/None           Enabled
        Auto
 8      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 9      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto

 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-3028P:4#show ports description
Command: show ports description

Port   State/          Settings             Connection           Address
        MDI       Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl    Learning
 -----  --------  ---------------------  ---------------------    --------
 1      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 Desc:
 2      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 Desc:
 3      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 Desc:
 4      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 Desc:
 5      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 Desc:
 6      Enabled   Auto/Disabled          LinkDown                 Enabled
        Auto
 Desc:

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

7

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	[<auth_portlist> | all] {admin_state [enable| disable] | max_learning_addr <max_lock_no 0-16> | lock_address_mode [DeleteOnTimeout | DeleteOnReset | Permanent]}
delete port_security entry	vlan_name <vlan_name 32> mac_address <macaddr> port <auth_port>
clear port_security_entry	port <auth_portlist>
show port_security	{ports <auth_portlist>}
enable port_security trap_log	
disable port_security trap_log	

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

config port_security ports

Purpose	Used to configure port security settings.
Syntax	**config port_security ports [<auth_portlist> | all] {admin_state [enable| disable] | max_learning_addr <max_lock_no 0-16> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the *<auth_portlist>* are affected.
Parameters	*<auth_portlist>* – Specifies a port or range of ports to be configured. *all* – Configure port security for all ports on the Switch. *admin_state [enable* | *disable]* – Enable or disable port security for the listed ports. *max_learning_addr <max_lock_no 0-16>* – Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports. *lock_address_mode [Permanent* | *DeleteOnTimout* | *DeleteOnReset]* – Indicates the method of locking addresses. The user has three choices: ▪ *Permanent* – The locked addresses will not age out. ▪ *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires (Aging Time is set using the FDB command). ▪ *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the port security:

```
DES-3028P:4#config port_security ports 1-5 admin_state
enable max_learning_addr 5 lock_address_mode
DeleteOnReset
Command: config port_security ports 1-5 admin_state
enable max_learning_addr 5 lock_address_mode
DeleteOnReset

Success.

DES-3028P:4#
```

delete port_security_entry

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

Example usage:

To delete a port security entry:

```
DES-3028P:4#delete port_security_entry vlan_name
default mac_address 00-01-30-10-2C-C7 port 6
Command: delete port_security_entry vlan_name
default mac_address 00-01-30-10-2C-C7 port 6

Success.

DES-3028P:4#
```

clear port_security_entry

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

Example usage:

To clear a port security entry by port:

```
DES-3028P:4# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DES-3028P:4#
```

show port_security

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

Example usage:

To display the port security configuration:

```
DES-3028P:4#show port_security ports 1-10
Command: show port_security ports 1-10

Port_security Trap/Log : Disabled

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

DES-3028P:4#
```

enable port_security trap_log

Purpose	Used to enable the trap log for port security.
Syntax	**enable port_security trap_log**
Description	This command, along with the **disable port_security trap_log,** will enable the sending of log messages to the Switch’s log and SNMP agent when the port security of the Switch has been triggered.
Parameters	None.
Restrictions	None.

Example usage:

To enable the port security trap log setting:

```
DES-3028P:4#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3028P:4#
```

disable port_security trap_log

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

Example usage:

To enable the port security trap log setting:

```
DES-3028P:4#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3028P:4#
```

8

NETWORK MANAGEMENT (SNMP) COMMANDS

The DES-3028/28G/28P/52/52P support the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. Users can specify which version of the SNMP users want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

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

Command	Parameters
create snmp user	<SNMP_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user	<SNMP_name 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included | excluded]
delete snmp view	<view_name 32> [all | oid]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community	<community_string 32>
show snmp community	<community_string 32>
config snmp engineID	<snmp_engineID 10-64>
show snmp engineID	
create snmp group	<groupname 32> {v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]} {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	<ipaddr> {v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]} <auth_string 32>

Command	Parameters
delete snmp host	<ipaddr>
show snmp host	<ipaddr>
create trusted_host	<ipaddr>| network<network_address>
delete trusted_host	[all | ipaddr<ipaddr>| network<network_address>]
show trusted_host	
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 rmon	
disable rmon	

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

create snmp user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	**create snmp user <SNMP_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}**
Description	The **create snmp user** 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	*<SNMP_name 32>* – An alphanumeric name of up to 32 characters that will identify the new SNMP user. *<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. *encrypted* – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose: *by_password* – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the auth_password below. This method is recommended. *by_key* – Requires the SNMP user to enter an encryption key for authentication and privacy. The key is defined by specifying the key in hex form below. This method is not recommended. *auth* – The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are: *md5* – Specifies that the HMAC-MD5-96 authentication level will be used. md5 may be utilized by entering one of the following:

create snmp user

	<auth password 8-16> – An alphanumeric sting of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host. *<auth_key 32-32>* – Enter an alphanumeric sting 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 sting 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 sting 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-3028P:4#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-3028P:4#
```

delete snmp user

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

Example usage:

To delete a previously entered SNMP user on the Switch:

```
DES-3028P:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-3028P:4#
```

show snmp user

Purpose	Used to display information about each SNMP username in the SNMP group username table.
Syntax	**show snmp user**
Description	The **show snmp user** command displays information about each SNMP username in the SNMP group username table.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the SNMP users currently configured on the Switch:

```
DES-3028P:4#show snmp user
Command: show snmp user

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

Total Entries: 1

DES-3028P:4#
```

create snmp view

Purpose	Used to assign views to community strings to limit which MIB objects and SNMP manager can access.
Syntax	**create snmp view <view_name 32> <oid> view_type [included | excluded]**
Description	The **create snmp view** command assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	*<view_name 32>* – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created. *<oid>* – The object ID that identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. *view type* – Sets the view type to be: • *included* – Include this object in the list of objects that an SNMP manager can access. • *excluded* – Exclude this object from the list of objects that an SNMP manager can access.

create snmp view	
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP view:

```
DES-3028P:4#create  snmp  view  dlinkview  1.3.6  view_type
included
Command:  create  snmp  view  dlinkview  1.3.6  view_type
included

Success.

DES-3028P:4#
```

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

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DES-3028P:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-3028P:4#
```

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

Example usage:

To display SNMP view configuration:

```
DES-3028P:4#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-3028P:4#
```

create snmp community

Purpose	Used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string: An 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. *read_write* or *read_only* level permission for the MIB objects accessible to the SNMP community.
Syntax	**create snmp community <community_string 32> view <view_name 32> [read_only | read_write]**
Description	The **create snmp community** command is used to create an SNMP community string and to assign access-limiting characteristics to this community string.
Parameters	*<community_string 32>* – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. *view <view_name 32>* – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. *read_only* – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch. *read_write* – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the SNMP community string “dlink:”

```
DES-3028P:4#create  snmp  community  dlink  view  ReadView
read_write
Command:  create  snmp  community  dlink  view  ReadView
read_write

Success.

DES-3028P:4#
```

delete snmp community

Purpose	Used to remove a specific SNMP community string from the Switch.
Syntax	**delete snmp community <community_string 32>**
Description	The **delete snmp community** 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-3028P:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-3028P:4#
```

show snmp community

Purpose	Used to display SNMP community strings configured on the Switch.
Syntax	**show snmp community {<community_string 32>}**
Description	The **show snmp community** 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-3028P:4#show snmp community
Command: show snmp community

SNMP Community Table

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

Total Entries: 3

DES-3028P:4#
```

config snmp engineID

Purpose	Used to configure a name for the SNMP engine on the Switch.
Syntax	**config snmp engineID <snmp_engineID>**
Description	The **config snmp engineID** command configures a name for the SNMP engine on the Switch.
Parameters	*<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-3028P:4#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DES-3028P:4#
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the Switch.
Syntax	**show snmp engineID**
Description	The **show snmp engineID** 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-3028P:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666
```

```
DES-3028P:4#
```

create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	**create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}**
Description	The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
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. *v1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • 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. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. *write_view* – Specifies that the SNMP group being created has write privileges. *notify_view* – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. *<view_name 32>* – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP group named "sg1:"

```
DES-3028P:4#create   snmp   group   sg1   v3   noauth_nopriv
read_view v1 write_view v1 notify_view v1
Command: create snmp group sg1 v3 noauth_nopriv read_view
v1 write_view v1 notify_view v1

Success.

DES-3028P:4#
```

delete snmp group

Purpose	Used to remove an SNMP group from the Switch.
Syntax	**delete snmp group <groupname 32>**
Description	The **delete snmp group** 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-3028P:4#delete snmp group sg1
Command: delete snmp group sg1

Success.

DES-3028P:4#
```

show snmp groups

Purpose	Used to display the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Syntax	**show snmp groups**
Description	The **show snmp groups** 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-3028P:4#show snmp groups
Command: show snmp groups
Vacm Access       Table Settings

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

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

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


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

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

Total Entries: 5

DES-3028P:4#
```

create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the Switch’s SNMP agent.
Syntax	**create snmp host <ipaddr> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] <auth_string 32>]**

create snmp host	
Description	The **create snmp host** command creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipaddr>* – The IP address of the remote management station that will serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • 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. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. *<auth_sting 32>* – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-3028P:4#create   snmp   host   10.48.74.100   v3
auth_priv public
Command: create snmp host 10.48.74.100 v3 auth_priv
public


Success.


DES-3028P:4#
```

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	The **delete snmp host** command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.

delete snmp host

Parameters	*<ipaddr>* – The IP address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an SNMP host entry:

```
DES-3028P:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DES-3028P:4#
```

show snmp host

Purpose	Used to display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp host {<ipaddr>}**
Description	The **show snmp host** 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-3028P:4#show snmp host
Command: show snmp host

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

Total Entries: 2

DES-3028P:4#
```

create trusted_host

Purpose	Used to create the trusted host.
Syntax	**create trusted_host <ipaddr>**
Description	The **create trusted_host** command creates the trusted host. The Switch allows users to specify up to ten IP addresses that are allowed to manage the Switch via in-band SNMP or TELNET based management software. These IP addresses must be members of the

create trusted_host

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

Example usage:

To create the trusted host:

```
DES-3028P:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DES-3028P:4#
```

create trusted_host network

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

Example usage:

To create the trusted host network:

```
DES-3028P:4#create trusted_host network 10.48.74.121/16
Command: create trusted_host network 10.48.74.121/16

Success.

DES-3028P:4#
```

show trusted_host

Purpose	Used to display a list of trusted hosts entered on the Switch using the **create trusted_host** command above.
Syntax	**show trusted_host**
Description	This command is used to display a list of trusted hosts entered on the Switch using the **create trusted_host** command above.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To display the list of trust hosts:

```
DES-3028P:4#show trusted_host
Command: show trusted_host

Management Stations

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

Total Entries: 1

DES-3028P:4#
```

delete trusted_host

Purpose	Used to delete a trusted host entry made using the **create trusted_host** command above.
Syntax	**delete trusted _host ipaddr <ipaddr>**
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-level users can issue this command.

Example usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DES-3028P:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DES-3028P:4#
```

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-level users can issue this command.

Example usage:

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

```
DES-3028P:4#delete trusted_host network 10.62.0.0/16
Command: delete trusted_host network 10.62.0.0/16
```

```
Success.

DES-3028P:4#
```

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-level users can issue this command.

Example usage:

To delete all trusted host entries:

```
DES-3028G:4# 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	The **enable snmp traps** command is used to enable SNMP trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SNMP trap support on the Switch:

```
DES-3028P:4#enable snmp traps
Command: enable snmp traps

Success.

DES-3028P:4#
```

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.

enable snmp authenticate traps

Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To turn on SNMP authentication trap support:

```
DES-3028P:4#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DES-3028P:4#
```

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	Only Administrator-level users can issue this command.

Example usage:

To view the current SNMP trap support:

```
DES-3028P:4#show snmp traps
Command: show snmp traps

SNMP Traps            : Enabled
Authenticate Traps    : Enabled

DES-3028P:4#
```

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-level users can issue this command.

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DES-3028P:4#disable snmp traps
Command: disable snmp traps

Success.

DES-3028P:4#
```

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-level users can issue this command.

Example usage:

To disable the SNMP authentication trap support:

```
DES-3028P:4#disable snmp authenticate traps
Command: disable snmp authenticate traps

Success.

DES-3028P:4#
```

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

Example usage:

To configure the Switch contact to "**MIS Department II**":

```
DES-3028P:4#config snmp system_contact MIS
Department II
Command: config snmp system_contact MIS Department
II

Success.

DES-3028P:4#
```

config snmp system_location	
Purpose	Used to enter a description of the location of the Switch.
Syntax	**config snmp system_location {<sw_location>}**
Description	The **config snmp system_location** command is used to enter a description of the location of the Switch. A maximum of 128 characters can be used.
Parameters	<*sw_location*> – A maximum of 128 characters is allowed. A NULL

config snmp system_location

	string is accepted if there is no location desired.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the Switch location for "**HQ 5F**":

```
DES-3028P:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3028P:4#
```

config snmp system_name

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

Example usage:

To configure the Switch name for "**DES-3028P Switch":**

```
DES-3028P:4#config   snmp   system_name   DES-3028P
Switch
Command: config snmp system_name DES-3028P Switch

Success.

DES-3028P:4#
```

enable rmon

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

Example Usage:

To enable RMON:

```
DES-3028P:4#enable rmon
Command: enable rmon

Success.

DES-3028P:4#
```

disable rmon

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

Example Usage:

To disable RMON:

```
DES-3028P:4#disable rmon
Command: disable rmon

Success.

DES-3028P:4#
```

9

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>} | cfg_fromTFTP <ipaddr> <path_filename 64> {increment}]
config firmware	image_id <int 1-2> [delete | boot_up]
show firmware information	
show config	[current_config | config_in_nvram]
upload	[cfg_toTFTP | log_toTFTP] <ipaddr> <path_filename 64>
enable autoconfig	
disable autoconfig	
show autoconfig	
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
config terminal _line	[default | <value 20-80>]
show terminal line	

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

download	
Purpose	Used to download and install new firmware or a Switch configuration file from a TFTP server.
Syntax	**download [firmware_fromTFTP <ipaddr> <path_filename 64> {image_id <int 1-2>} | cfg_fromTFTP <ipaddr> <path_filename 64> {increment}]**
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	*firmware_fromTFTP* – Download and install new firmware on the Switch from a TFTP server. *cfg_fromTFTP* – Download a switch configuration file from a TFTP server. *<ipaddr>* – The IP address of the TFTP server. *<path_filename>* – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3028.had. *image_id <int 1-2>* – Specify the working section ID. The Switch can hold two firmware versions for the user to select from, which are specified by section ID. *increment* – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
Restrictions	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-3028P:4#download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt
Command: download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt

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

DES-3028P:4#
DES-3028P:4##--------------------------------------------------------------------
DES-3028P:4##                   DES-3028P Configuration
DES-3028P:4##
DES-3028P:4##                   Firmware: Build 2.00.B23
DES-3028P:4##  Copyright(C) 2009 D-Link Corporation. All rights reserved.
DES-3028P:4##--------------------------------------------------------------------
DES-3028P:4#
DES-3028P:4#
DES-3028P:4## BASIC
DES-3028P:4#
DES-3028P:4#config serial_port baud_rate 9600 auto_logout 10_minutes
Command: config serial_port baud_rate 9600 auto_logout 10_minutes
```

The download configuration command will initiate the loading of the various settings in the order listed in the configuration file. When the file has been successfully loaded the message "End of configuration file for DES-3028P" appears followed by the command prompt.

```
DES-3028P:4#disable authen_policy
Command: disable authen_policy

Success.

DES-3028P:4#
```

config firmware

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

Example usage:

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

```
DES-3028P:4# config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DES-3028P:4#
```

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

Example usage:

To display the current firmware information on the Switch:

```
DES-3028P:4#show firmware information
Command: show firmware information

ID  Version   Size(B)     Update Time          From                   User
--  --------  -------  -------------------  --------------------    -------------
*1  2.00.B23  1861680  0000/00/00 05:22:22  10.73.21.1(CONSOLE)      Anonymous
 2  1.00.B32  1533156  0000/00/00 00:03:03  172.18.215.217(CONSOLE)  Anonymous

'*'       : Boot up firmware
(SSH)     : Firmware update through SSH
(WEB)     : Firmware update through WEB
(SIM)     : Firmware update through Single IP Management
(SNMP)    : Firmware update through SNMP
(TELNET)  : Firmware update through TELNET
(CONSOLE) : Firmware update through CONSOLE

DES-3028P:4#
```

show config	
Purpose	Used to display the current or saved version of the configuration settings of the switch.
Syntax	**show config [current_config | config_in_nvram]**
Description	Use this command 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). The configuration settings are listed by category in the following order:

show config	
	1. Basic (serial port, Telnet and web management status) 2. storm control 3. IP group management 4. Syslog 5. QoS 6. port mirroring 7. traffic segmentation 8. port 9. port lock 10. 8021x 11. SNMPv3 12. management (SNMP traps RMON) 13. VLAN 14. FDB (forwarding data base) 15. MAC address table notification 16. STP 17. SSH 18. SSL 19. ACL 20. SNTP 21. IP route 22. LACP 23. ARP 24. IP 25. IGMP snooping 26. access authentication control (TACACS etc.) 27. PoE 28. Bandwidth 29. Time_range 30. GM 31. safeguard_engine 32. Banner_promp 33. SMTP 34. AAA 35. DHCP_Relay
Parameters	*current_config* – Entering this parameter will display configurations entered without being saved to NVRAM. *config_in_NVRAM* – Entering this parameter will display configurations entered and saved to NVRAM.
Restrictions	None.

Example usage:

To view the current configuration settings:

```
DES-3028P:4#show config current_config
Command: show config current_config

-------------------------------------------------------------------
#                      DES-3028P Configuration
#
#                      Firmware: Build 2.00.B23
#        Copyright(C) 2009 D-Link Corporation. All rights reserved.
#-------------------------------------------------------------------



# BASIC

config serial_port baud_rate 9600 auto_logout never
# ACCOUNT LIST

# ACCOUNT END

# PASSWORD ENCRYPTION
disable password encryption
config terminal_line default
enable clipaging

# STORM

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

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

Example usage:

To upload a configuration file:

```
DES-3028P:4#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-3028P:4#
```

enable autoconfig

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

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

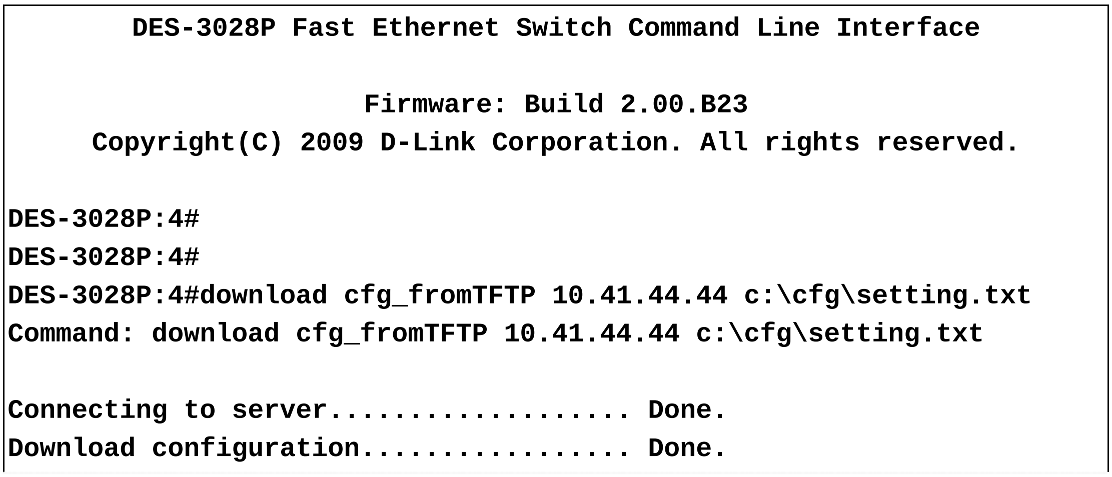
Example usage:

To enable auto configuration on the Switch:

```
DES-3028P:4#enable autoconfig
Command: enable autoconfig

Success.

DES-3028P:4#
```

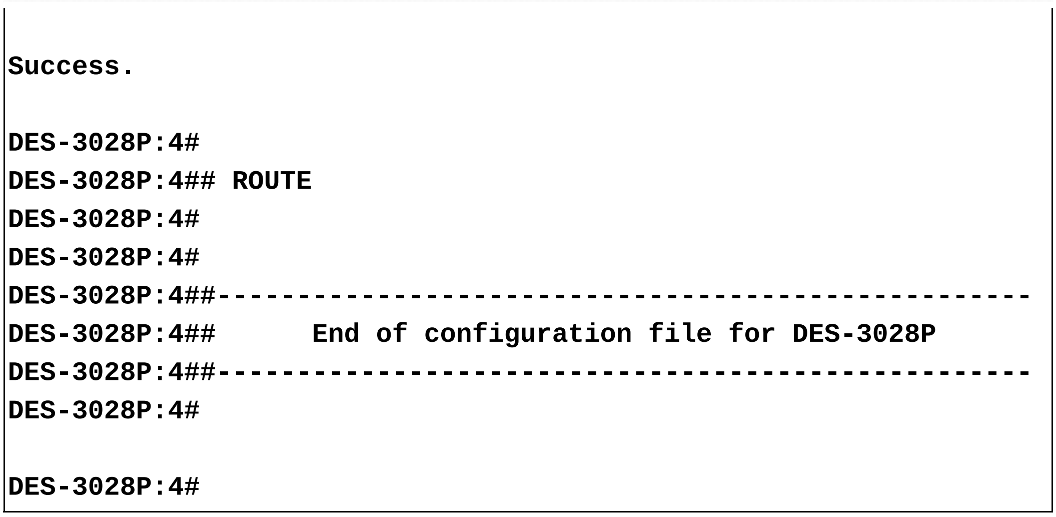
When autoconfig is enabled and the Switch is rebooted, the normal login screen will appear for a few moments while the autoconfig request (i.e. download configuration) is initiated. The console will then display the configuration parameters as they are loaded from the configuration file specified in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

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



```
              DES-3028P Fast Ethernet Switch Command Line Interface

                           Firmware: Build 2.00.B23
            Copyright(C) 2009 D-Link Corporation. All rights reserved.

DES-3028P:4#
DES-3028P:4#
DES-3028P:4#download cfg_fromTFTP 10.41.44.44 c:\cfg\setting.txt
Command: download cfg_fromTFTP 10.41.44.44 c:\cfg\setting.txt

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

The very end of the autoconfig process appears like this:



```

Success.

DES-3028P:4#
DES-3028P:4## ROUTE
DES-3028P:4#
DES-3028P:4#
DES-3028P:4##---------------------------------------------------
DES-3028P:4##      End of configuration file for DES-3028P
DES-3028P:4##---------------------------------------------------
DES-3028P:4#

DES-3028P:4#
```

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

disable autoconfig	
Purpose	Use this to deactivate auto configuration from DHCP.
Syntax	**disable autoconfig**
Description	This instructs the Switch not to accept auto configuration instruction from the DHCP server. This does not change the IP settings of the Switch. The ipif settings will continue as DHCP client until changed with the **config ipif** command.
Parameters	None.
Restrictions	None.

Example usage:

To stop the auto configuration function:

```
DES-3028P:4#disable autoconfig
Command: disable autoconfig

Success.

DES-3028P:4#
```

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 auto configuration function.
Parameters	None.
Restrictions	None.

Example usage:

To display the autoconfig status:

```
DES-3028P:4#show autoconfig
Command: show autoconfig

Autoconfig State:  Disabled

DES-3028P:4#
```

ping

Purpose	Used to test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}**
Description	The ping 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	*<ipaddr>* – Specifies the IP address of the host. *times <value 1-255>* – The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0. *timeout <sec 1-99>* – Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DES-3028P:4#ping 10.48.74.121 times 4
Command: ping 10.48.74.121

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

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

DES-3028P:4#
```

config terminal line

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

Example usage:

To configure the terminal line:

```
DES-3028P:4# config terminal_line 30
Command: config terminal_line 30

Success.

 DES-3028P:4#
```

show terminal line

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

Example usage:

To show the terminal line:

```
DES-3028P:4# show terminal_line
Command: show terminal_line

Current terminal line number : 30

 DES-3028P:4#
```

10

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

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-3028P:4#show packet ports 2
Command: show packet ports 2

Port Number : 2
 Frame Size    Frame Counts  Frames/sec    Frame Type   Total      Total/sec
 ------------  ------------  ----------    ----------   ---------  ---------
 64            0             0             RX Bytes     0          0
 65-127        0             0             RX Frames    0          0
 128-255       0             0
 256-511       0             0             TX Bytes     0          0
 512-1023      0             0             TX Frames    0          0
 1024-1518     0             0

 Unicast RX    0             0
 Multicast RX  0             0
 Broadcast RX  0             0

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

show error ports

Purpose	Used to display the error statistics for a range of ports.
Syntax	**show error ports <portlist>**
Description	This command 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-3028P:4#show error ports 3
Command: show error ports 3

Port Number : 3
                 RX Frames                                  TX Frames
                 ---------                                  ---------
 CRC Error       0                    Excessive Deferral    0
 Undersize       0                    CRC Error             0
 Oversize        0                    Late Collision        0
 Fragment        0                    Excessive Collision   0
 Jabber          0                    Single Collision      0
 Drop Pkts       0                    Collision             0

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

show utilization	
Purpose	Used to display real-time 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	*cpu* – Entering this parameter will display the current cpu utilization of the Switch. *ports* – Entering this parameter will display the current port utilization of the Switch. ▪ *<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the port utilization statistics:

```
DES-3028P:4#show utilization ports
Command: show utilization ports

Port     TX/sec     RX/sec    Util      Port     TX/sec     RX/sec    Util
 ----   ---------- ---------- ----       ----   ---------- ---------- ----
 1      0          0           0         22     0          0           0
 2      0          0           0         23     0          0           0
 3      0          0           0         24     0          0           0
 4      0          0           0         25     0          0           0
 5      0          0           0         26     0          0           0
 6      0          0           0         27     0          0           0
 7      0          37          1         28     0          0           0
 8      0          0           0
 9      0          0           0
 10     0          0           0
 11     36         0           1
 12     0          0           0
 13     0          0           0
 14     0          0           0
 15     0          0           0
 16     0          0           0
 17     0          0           0
 18     0          0           0
 19     0          0           0
 20     0          0           0
 21     0          0           0
 CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the current CPU utilization:

```
DES-3028P:4#show utilization cpu
Command: show utilization cpu

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

DES-3028P:4#
```

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-level users can issue this command.

Example usage:

To clear the counters:

```
DES-3028P:4#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

DES-3028P:4#
```

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-level users can issue this command.

Example usage:

To clear the log information:

```
DES-3028P:4#clear log
Command: clear log

Success.

DES-3028P:4#
```

show log

Purpose	Used to display the switch history log.
Syntax	**show log {index <value_list X-Y>}**
Description	This command will display the contents of the Switch’s history log.
Parameters	*index <value_list X-Y>* – This command will display the history log, beginning and ending at the value specified by the user in the *<value_list X-Y>* field. If no parameter is specified, all history log entries will be displayed.

show log

Restrictions	None.

Example usage:

To display the switch history log**:**

```
DES-3028P:4#show log index 1-5
Command: show log index 1-5

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

DES-3028P:4#
```

enable syslog

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

Example usage:

To the syslog function on the Switch:

```
DES-3028P:4#enable syslog
Command: enable syslog

Success.

DES-3028P:4#
```

disable syslog

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

Example usage:

To disable the syslog function on the Switch:

```
DES-3028P:4#disable syslog
Command: disable syslog

Success.

DES-3028P:4#
```

show syslog

Purpose	Used to display the syslog protocol status as enabled or disabled.
Syntax	**show syslog**
Description	The **show syslog** 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-3028P:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-3028P:4#
```

create syslog host

Purpose	Used to create a new syslog host.
Syntax	**create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]**
Description	The **create syslog host** command is used to create a new syslog 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 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

create syslog host

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

Example usage:

To create syslog host:

```
DES-3028P:4#create  syslog  host  1  severity  all
facility local0
Command: create syslog host 1 severity all facility
local0

Success.

DES-3028P:4#
```

config syslog host

<table>
<tr><td>Purpose</td><td>Used to configure the syslog protocol to send system log data to a remote host.</td></tr>
<tr><td>Syntax</td><td><b>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]</b></td></tr>
<tr><td>Description</td><td>The <b>config syslog host</b> command is used to configure the syslog protocol to send system log information to a remote host.</td></tr>
<tr><td>Parameters</td><td><i>&lt;index 1-4&gt;</i> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.
<i>ipaddress <ipaddr&gt;</i> – Specifies the IP address of the remote host where syslog messages will be sent.
<i>severity</i> – Severity level indicator. These are described in the following:
<b>Bold</b> font indicates that the corresponding severity level is currently supported on the Switch.
<table>
<tr><th>Numerical Code</th><th>Severity</th></tr>
<tr><td>0</td><td>Emergency: system is unusable</td></tr>
<tr><td>1</td><td>Alert: action must be taken immediately</td></tr>
<tr><td>2</td><td>Critical: critical conditions</td></tr>
<tr><td>3</td><td>Error: error conditions</td></tr>
<tr><td><b>4</b></td><td><b>Warning: warning conditions</b></td></tr>
<tr><td>5</td><td>Notice: normal but significant condition</td></tr>
<tr><td><b>6</b></td><td><b>Informational: informational messages</b></td></tr>
<tr><td>7</td><td>Debug: debug-level messages</td></tr>
</table>
<i>informational</i> – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above.
<i>warning</i> – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above.
<i>all</i> – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host.
<i>facility</i> – 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.</td></tr>
</table>

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

Parameters	*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-level users can issue this command.

Example usage:

To configure a Syslog host:

```
DES-3028P:4#config syslog host 1 severity all facility
local0
Command: config syslog host all severity all facility
local0

Success.

DES-3028P:4#
```

Example usage:

To configure a Syslog host for all hosts:

```
DES-3028P:4#config syslog host all severity all facility
local0
Command: config syslog host all severity all facility
local0

Success.

DES-3028P:4#
```

delete syslog host

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

Example usage:

To delete a previously configured syslog host:

```
DES-3028P:4#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3028P:4#
```

show syslog host

Purpose	Used to display the syslog hosts currently configured on the Switch.
Syntax	**show syslog host {<index 1-4>}**
Description	The **show syslog host** 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-3028P:4#show syslog host
Command: show syslog host

Syslog Global State: Disabled

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

Total Entries : 3

DES-3028P:4#
```

config log_save_timing

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

Example usage:

To configure the time interval as every 30 minutes for saving log files**:**

```
DES-3028P:4#config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

DES-3028P:4#
```

show log_save_timing

Purpose	Used to display the method configured for saving log files to the switch’s flash memory.
Syntax	**show log_save_timing**
Description	The **show log_save_timing** command allows the user to view the time method configured for saving log files to the switch’s flash memory.
Parameters	None.
Restrictions	None.

Example usage:

To display the time interval for saving log files**:**

```
DES-3028P:4#show log_save_timing
Command: show log_save_timing

Saving log method: time_interval
                  Interval : 30

DES-3028P:4#
```

11

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 BDPU 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) 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>*).

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

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

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

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

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

c) 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> | fbpdu [enable | disable] | lbd [enable | disable] | lbd_recover_timer [0 | <value 60-1000000>]}
config stp ports	<portlist> {externalCost [auto | <value 1-200000000>] |hellotime <value 1-2> | migrate [yes|no] |edge [true|false|auto]| restricted_role [true|false] |restricted_tcn [true|false]| p2p [true|false|auto] |state [enable|disable]|lbd [enable|disable]|fbpdu [enable|disable]}
create stp instance_id	<value 1-4>
config stp instance _id	<value 1-4> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id	<value 1-4>
config stp priority	<value 0-61440> instance_id <value 0-4>
config stp mst_config_id	{revision_level <int 0-65535> | name <string>}
config stp mst_ports	<portlist> instance_id <value 0-4> {internalCost [auto | value 1-200000000] | priority <value 0-240>}
show stp	

Command	Parameters
show stp ports	{<portlist>} {instance <value 0-4>}
show stp instance	{<value 0-4>}
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-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DES-3028P:4#enable stp
Command: enable stp

Success.

DES-3028P:4#
```

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-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DES-3028P:4#disable stp
Command: disable stp

Success.

DES-3028P:4#
```

config stp version

Purpose	Used to globally set the version of STP on the Switch.
Syntax	**config stp version [mstp | rstp | stp]**
Description	This command allows the user to choose the version of the spanning tree to be implemented on the Switch.

config stp version

Parameters	*mstp* – Selecting this parameter will set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. *rstp* – Selecting this parameter will set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *stp* – Selecting this parameter will set the Spanning Tree Protocol (STP) globally on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#config stp version mstp
Command: config stp version mstp

Success.

DES-3028P:4#
```

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] | lbd [enable | disable] | lbd_recover_timer [0 | <value 60-1000000>]}**
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	*maxage <value 6-40>* – 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. *maxhops <value 6-40>* – 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 BDPU 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. *hellotime <value 1-2>* – 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. **NOTE:** In MSTP, the spanning tree is configured by port and therefore, the *hellotime* must be set using the *configure stp ports* command for switches utilizing the Multiple Spanning Tree Protocol. *forwarddelay <value 4-30>* – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may

config stp

	choose a time between 4 and 30 seconds. The default is 15 seconds. *txholdcount <1-10>* – The maximum number of BPDU Hello packets transmitted per interval. Default value = 6. *fbpdu [enable* | *disable]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *enable*. *lbd [enable* | *disable]* – Enabling this feature temporarily block STP on the Switch when a BPDU packet has been looped back to the switch. When the Switch detects its own BPDU packet coming back, it signifies a loop on the network. STP will automatically be blocked and an alert will be sent to the administrator. The LBD STP port will restart (change to discarding state) when the **LBD Recover Time** times out. The default is enabled. *lbd_recover_timer [0* | *<value 60-1000000>]* – This field will set the time the STP port will wait before recovering the STP state set. 0 will denote that the LBD will never time out or restart until the administrator personally changes it. The user may also set a time between 60 and 1000000 seconds. The default is 60 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DES-3028P:4#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

DES-3028P:4#
```

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	**<portlist> {externalCost [auto | <value 1-200000000>] |hellotime <value 1-2> | migrate [yes|no] |edge [true|false|auto]| restricted_role [true|false] |restricted_tcn [true|false]| p2p [true|false|auto] |state [enable|disable]|lbd [enable|disable]|fbpdu [enable|disable]}**
Description	This command is used to create and configure STP for a group of ports.
Parameters	*<portlist>* – Specifies a range of ports to be configured. *externalCost* – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *auto*. *auto* – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. *<value 1-200000000>* – Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. *hellotime <value 1-2>* – The time interval between transmission of configuration messages by the designated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and 2 seconds. The default is 2 seconds. *migrate [yes* | *no]* – Setting this parameter as "*yes*" will set the ports to send out BDPU packets to other bridges, requesting information on their STP setting If the

config stp ports	
	Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1D STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1D network connects to an 802.1w or 802.1s enabled network. Migration should be set as *yes* on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment. *edge [true* | *false* | *auto] – true* designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status. *p2p [true* | *false* | *auto] – true* indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were *true*. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *false*. The default setting for this parameter is *auto*. *state [enable* | *disable]* – Allows STP to be enabled or disabled for the ports specified in the port list. The default is *enable*. *restricted_role* – To decide if this is to be selected as the Root Port. The default value is false. *restricted_tcn* – To decide if this port is to propagate topology change. The default value is false. *lbd [enable* | *disable]* – Used to enable or disable the loop-back detection function on the switch for the ports configured above in the *config stp* command. *fbpdu [enable* | *disable]* – When enabled, this allows the forwarding of STP BPDU packets from other network devices when STP is disabled in the specified ports. If users want to enable Forwarding BPDU on a per port basis, the following settings must first be in effect: 1. STP must be globally disabled and 2. Forwarding BPDU must be globally enabled. To globally disable STP, use the **disable stp** command, to globally enable fbpdu, use the **config stp** command. The default is *enable.*
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#config stp ports 1-2 externalCost auto hellotime 2 migrate
yes state
 enable
Command: config stp ports 1-2 externalCost auto hellotime 2 migrate
yes state en
able

DES-3028P:4#
```

create stp instance_id

Purpose	Used to create a STP instance ID for MSTP.
Syntax	**create stp instance_id <value 1-4>**
Description	This command allows the user to create a STP instance ID for the Multiple Spanning Tree Protocol. There are 5 STP instances on the Switch (one internal CIST, unchangeable) and the user may create up to 4 instance IDs for the Switch.
Parameters	*<value 1-4>* – Enter a value between 1 and 4 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a spanning tree instance 2:

```
DES-3028P:4#create stp instance_id 2
Command: create stp instance_id 2

Success.

DES-3028P:4#
```

config stp instance_id

Purpose	Used to add or delete an STP instance ID.
Syntax	**config stp instance_id <value 1-4> [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 *instance_id*. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 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 *instance_id* must be mapped identically, and have the same configuration *revision_level* number and the same *name*.
Parameters	*<value 1-4>* – Enter a number between 1 and 4 to define the *instance_id*. The Switch supports 16 STP instances with one unchangeable default instance ID set as *0*. *add_vlan* – Along with the *vid_range <vidlist>* parameter, this command

config stp instance_id

	will add VIDs to the previously configured STP *instance_id.* *remove_vlan* – Along with the *vid_range* <*vidlist*> parameter, this command will remove VIDs to the previously configured STP *instance_id.* <*vidlist*> – 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-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DES-3028P:4#config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.

DES-3028P:4#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DES-3028P:4#config stp instance_id 2 remove_vlan 10
Command : config stp instance_id 2 remove_vlan 10

Success.

DES-3028P:4#
```

delete stp instance_id

Purpose	Used to delete a STP instance ID from the Switch.
Syntax	**delete stp instance_id <value 1-4>**
Description	This command allows the user to delete a previously configured STP instance ID from the Switch.
Parameters	<*value 1-4*> – Enter a value between 1 and 4 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete STP instance ID 2 from the Switch.

```
DES-3028P:4#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DES-3028P:4#
```

config stp priority

Purpose	Used to update the STP instance configuration
Syntax	**config stp priority <value 0-61440> instance_id <value 0-4>**
Description	This command is used to update the STP instance configuration settings on the Switch. The MSTP will utilize the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions will instruct the Switch to give precedence to the selected *instance_id* for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	*priority <value 0-61440>* – Select a value between 0 and 61440 to specify the priority for a specified instance ID for forwarding packets. The lower the value, the higher the priority. This entry must be divisible by 4096. *instance_id <value 0-4>* – Enter the value corresponding to the previously configured instance ID of which the user wishes to set the priority value. An instance id of *0* denotes the default *instance_id* (CIST) internally set on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#config stp priority 4096 instance_id 2
Command : config stp priority 4096 instance_id 2

Success.

DES-3028P:4#
```

config stp mst_config_id

Purpose	Used to update the MSTP configuration identification.
Syntax	**config stp mst_config_id {revision_level <int 0-65535> | name <string 32>}**
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 *revision_level* and *name* will be considered as part of the same MSTP region.
Parameters	*revision_level <int 0-65535>* – Enter a number between 0 and 65535 to identify the MSTP region. This value, along with the name will identify the MSTP region configured on the Switch. The default setting is *0*. *name <string 32>* – Enter an alphanumeric string of up to 32 characters to uniquely identify the MSTP region on the Switch. This *name*, along with the *revision_level* value will identify the MSTP region configured on the Switch. If no *name* is entered, the default name will be the MAC address of the device.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#config  stp  mst_config_id  revision_level  10
name Trinity
Command : config stp mst_config_id revision_level 10 name
Trinity

Success.

DES-3028P:4#
```

config stp mst_ports

Purpose	Used to update the port configuration for a MSTP instance.
Syntax	**config stp mst_ports <portlist> instance_id <value 0-4> {internalCost [auto | <value 1-20000000>] priority <value 0-240>**
Description	This command will update the port configuration for a STP *instance_id*. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *instance_id <value 0-4>* – Enter a numerical value between 0 and 4 to identify the *instance_id* previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree). *internalCost* – This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *auto*. There are two options: *auto* – Selecting this parameter for the internalCost will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. *value 1-200000000* – Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower *internalCost* represents a quicker transmission. *priority <value 0-240>* – Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#config  stp  mst_ports  1-5  instance_id  2
internalCost auto priority 16
Command  :  config  stp  mst_ports  1-5  instance_id  2
internalCost auto priority 16

Success.

DES-3028P:4#
```

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-3028P:4#show stp
Command: show stp

STP Bridge Global Settings
 ---------------------------
 STP Status         : Enabled
 STP Version        : STP compatible
 Max Age            : 20
 Hello Time         : 2
 Forward Delay      : 15
 Max Hops           : 20
 TX Hold Count      : 6
 Forwarding BPDU    : Enabled
 Loopback Detection : Enabled
 LBD Recover Time   : 60

DES-3028P:4#
```

Status 2 : STP enabled for RSTP

```
DES-3028P:4#show stp
Command: show stp

STP Bridge Global Settings
 ---------------------------
STP Status                 : Enabled
STP Version                : RSTP
Max Age                    : 20
Hello Time                 : 2
Forward Delay              : 15
Max Hops                   : 20
TX Hold Count              : 6
Forwarding BPDU            : Enabled
Loopback Detection         : Enabled
LBD Recover Time           : 60

DES-3028P:4#
```

Status 3 : STP enabled for MSTP

```
DES-3028P:4#show stp
Command: show stp
```

```
STP Bridge Global Settings
 ---------------------------
STP Status                  : Enabled
STP Version                 : MSTP
Max Age                     : 20
Forward Delay               : 15
Max Hops                    : 20
TX Hold Count               : 6
Forwarding BPDU             : Enabled
Loopback Detection          : Enabled
LBD Recover Time            : 60

DES-3028P:4#
```

show stp ports

Purpose	Used to display the Switch’s current STP ports configuration.
Syntax	**show stp ports {<portlist>} {instance <value 0-4>}**
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-3028P:4#show stp ports
Command: show stp ports

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

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

show stp instance_id

Purpose	Used to display the Switch’s STP instance configuration
Syntax	**show stp instance_id <value 0-4>**
Description	This command displays the Switch’s current STP Instance Settings and the STP Instance Operational Status.
Parameters	*<value 0-4>* – Enter a value defining the previously configured *instance_id* on the Switch. An entry of *0* will display the STP

show stp instance_id	
	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-3028P:4#show stp instance 0
Command: show stp instance 0

STP Instance Settings
 ---------------------------
 Instance Type      : CIST
 Instance Status    : Enabled
 Instance Priority  : 32768(bridge priority : 32768, sys ID ext : 0 )

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

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

show stp mst_config_id	
Purpose	Used to display the MSTP configuration identification.
Syntax	**show stp mst_config_id**
Description	This command 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-3028P:4#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
----------------------------------------------------------

Configuration Name : [00:53:13:1A:33:24]  Revision Level :0
MSTI ID     VID list
-------     -----------
  CIST        2-4094
   1            1

DES-3028P:4#
```

12

FORWARDING DATABASE COMMANDS

The layer 2 forwarding database commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

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

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

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

Example usage:

To create a unicast MAC FDB entry**:**

```
DES-3028P:4#create  fdb  default  00-00-00-00-01-02
port 5
Command: create fdb default 00-00-00-00-01-02 port
5

Success.

DES-3028P:4#
```

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

Example usage:

To create multicast MAC forwarding**:**

```
DES-3028P:4#create  multicast_fdb  default  01-00-00-
00-00-01
Command:  create  multicast_fdb  default  01-00-00-00-
00-01

Success.

DES-3028P:4#
```

config multicast_fdb

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

Example usage:

To add multicast MAC forwarding:

```
DES-3028P:4#config multicast_fdb default 01-00-00-00-00-
01 add 1-5
Command: config multicast_fdb default 01-00-00-00-00-01
add 1-5

Success.

DES-3028P:4#
```

config fdb aging_time

Purpose	Used to set the aging time of the forwarding database.
Syntax	config fdb aging_time <sec 10-1000000>
Description	The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 10 to 1000000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the Switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a switch.
Parameters	<sec 10-1000000> – The aging time for the MAC address forwarding database value. The value in seconds may be between 10 and 1000000 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the fdb aging time:

```
DES-3028P:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3028P:4#
```

delete fdb

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

Example usage:

To delete a permanent FDB entry:

```
DES-3028P:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3028P:4#
```

To delete a multicast FDB entry:

```
DES-3028P:4#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DES-3028P:4#
```

clear fdb

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

Example usage:

To clear all FDB dynamic entries**:**

```
DES-3028P:4#clear fdb all
Command: clear fdb all
```

```
Success.

DES-3028P:4#
```

show multicast_fdb

Purpose	Used to display the contents of the Switch's multicast forwarding database.
Syntax	**show mulitcast_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-3028P:4#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

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

Total Entries  : 1

DES-3028P:4#
```

show fdb

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

Example usage:

To display unicast MAC address table:

```
DES-3028P:4#show fdb
Command: show fdb

Unicast MAC Address Ageing Time = 300

VID   VLAN Name      MAC Address           Port        Type
----  ------------  ----------------       ------      ----------------
1        default     00-00-51-43-70-00       10          Dynamic
1        default     00-00-5E-00-01-01       10          Dynamic
1        default     00-00-74-60-72-2D       10          Dynamic
1        default     00-00-81-05-00-80       10          Dynamic
1        default     00-00-81-05-02-00       10          Dynamic
1        default     00-00-81-48-70-01       10          Dynamic
1        default     00-00-E2-4F-57-03       10          Dynamic
1        default     00-00-E2-61-53-18       10          Dynamic
1        default     00-00-E2-6B-BC-F6       10          Dynamic
1        default     00-00-E2-7F-6B-53       10          Dynamic
1        default     00-00-E2-82-7D-90       10          Dynamic
1        default     00-00-F8-7C-1C-29       10          Dynamic
1        default     00-01-02-03-04-00      CPU          Self
1        default     00-01-02-03-04-05       10          Dynamic
1        default     00-01-30-10-2C-C7       10          Dynamic
1        default     00-01-30-FA-5F-00       10          Dynamic
1        default     00-02-3F-63-DD-68       10          Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config multicast port_filtering_mode

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

Example usage:

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

```
DES-3028P:4#config multicast port_filtering_mode 1-4
forward_unregistered_groups
Command: config multicast port_filtering_mode 1-4
forward_unregistered_groups

Success.

DES-3028P:4#
```

show multicast port_filtering_mode

Purpose	Used to show the multicast packet filtering mode on a port per port basis.
Syntax	**show multicast port_filtering_mode**
Description	This command will display the current multicast packet filtering mode for specified ports on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the multicast port filtering mode for all ports:

```
DES-3028P:4#show multicast port_filtering_mode
Command: show multicast port_filtering_mode

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

DES-3028P:4#
```

13

BROADCAST STORM CONTROL COMMANDS

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

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

The 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 64-1000000> | time_interval <secs 5-30> | countdown [<minutes 0>| <minutes 5-30>]}
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 64-1000000> | time_interval <secs 5-30> | countdown [<minutes 0> | <minutes 5-30>]}**
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	*<portlist>* – Used to specify a range of ports to be configured for traffic control. *all* – Specifies all ports are to be configured for traffic control on the Switch. *broadcast [enable | disable]* – Enables or disables broadcast storm control. *multicast [enable | disable]* – Enables or disables multicast storm control. *unicast [enable | disable]* – Enables or disables Unknown unicast traffic control. *action* – Used to configure the action taken when a storm control has been

config traffic control	
	detected on the Switch. The user has two options: *drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. *shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Storm continues, the port will be placed in Rest mode and is no longer operational until (1) auto-recovery after 5 minutes or (2) the user manually resets the port using the **config ports 1 state disable** and **config ports 1 state enable** command. Choosing this option obligates the user to configure the *time_interval* field as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring. *threshold <value 64-1000000>* – The upper threshold at which the specified traffic control is switched on. The *<value>* is the number of broadcast/multicast/Unknown unicast packets, in Kbits per second (Kbit/sec), received by the Switch that will trigger the storm traffic control measures. The default setting is 64 Kbit/sec. *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. *secs 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. 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. *minutes 0* – 0 is the default setting for this field and 0 will denote that the port will never shutdown. *minutes 5-30* – Select a time from 5 to 30 minutes that the Switch will wait before shutting down. Once this time expires and the port is still experiencing packet storms, the port will be placed in rest mode and can only be manually recovered using the config ports command mentioned previously in this manual.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4# config traffic control 1-12 broadcast enable
action shutdown threshold 64 countdown 10 time_interval 10
Command: config traffic control 1-12 broadcast enable
action shutdown threshold 64 countdown 10 time_interval 10


Success.


DES-3028P:4#
```

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	*<portlist>* – Used to specify port or list of ports for which to display traffic control settings. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display traffic control setting for ports 1-4:

```
DES-3028P:4#show traffic control 1-4
Command: show traffic control 1-4

Traffic Storm Control Trap :[None]

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

Total Entries  : 4

DES-3028P:4#
```

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 will 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 control** command is set as **shutdown**).
Parameters	*none* – No notification will be generated or sent when a packet storm control is detected by the Switch. *storm _occurred* – A notification will be generated and sent when a packet storm has been detected by the Switch. *storm_cleared* – A notification will be generated and sent when a packet storm has been cleared by the Switch. *both* – A notification will be generated and sent when a packet storm has been detected and cleared by the Switch.
Restrictions	Only Administrator-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-3028P:4# config traffic trap both
Command: config traffic trap both

Success.

DES-3028P:4#
```

14

CoS Commands

The DES-3028/28G/28P/52/52P supports 802.1p priority queuing. The Switch has four priority queues. These priority queues are numbered from 3 (Class 3) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

- Priority 0 is assigned to the Switch's Q1 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q0 queue.
- Priority 3 is assigned to the Switch's Q1 queue.
- Priority 4 is assigned to the Switch's Q2 queue.
- Priority 5 is assigned to the Switch's Q2 queue.
- Priority 6 is assigned to the Switch's Q3 queue.
- Priority 7 is assigned to the Switch's Q3 queue.

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

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

Command	Parameters
config bandwidth_control	[<portlist>] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit <value 64-1024000>]}
show bandwidth_control	<portlist>
config scheduling	<class_id 0-3> {weight <value 1-55>}
config scheduling_mechanism	[strict | weight_fair]
show scheduling	
show scheduling_mechanism	
config 802.1p user_priority	<priority 0-7> <class_id 0-3>
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> | all] <priority 0-7>
show 802.1p default_priority	<portlist>
config cos mapping port	[<portlist> | all] [none | {port_mapping | ethernet [802.1p | mac_mapping] | ip [tos | dscp]}]
show cos mapping	{port <portlist> }
config cos port_mapping	[class [0(1) | 3(2)] [<portlist> | all]
show cos port_mapping	{port <portlist> }
config cos mac_mapping	destination_addr <macaddr> [class <class_id 0-3>]
show cos mac_mapping	{destination_addr < macaddr > }
config cos tos value	<value 0-7> [class <class_id 0-3>]
show cos tos	{value <value 0-7>}
config dscp_mapping	dscp_value <value 0-63> [class <class_id 0-3>]
show dscp_mapping	{dscp_value <value 0-63> }

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

config bandwidth_control

Purpose	Used to configure bandwidth control on a port by-port basis.
Syntax	**config bandwidth_control [<portlist>] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit <value 64-1024000>]}**
Description	The **config bandwidth_control** command is used to configure bandwidth on a port by-port basis.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *rx_rate* – Specifies that one of the parameters below (*no_limit* or <*value 64-1024000*>) will be applied to the rate at which the above specified ports will be allowed to receive packets ▪ *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ *<value 64-1024000>* – Specifies the traffic limit, in Kbits, that the above ports will be allowed to receive. *tx_rate* – Specifies that one of the parameters below (*no_limit* or <*value 64-1024000*>) will be applied to the rate at which the above specified ports will be allowed to transmit packets. ▪ *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ *<value 64-1024000>* – Specifies the traffic limit, in Kbits, that the above ports will be allowed to receive.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DES-3028P:4#config bandwidth_control 1 rx_rate 64
Command: config bandwidth_control 1 rx_rate 64

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

Success.


DES-3028P:4#
```

show bandwidth_control

Purpose	Used to display the bandwidth control table.
Syntax	**show bandwidth_control {<portlist>}**
Description	The **show bandwidth_control** 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 bandwidth control settings:

```
DES-3028P:4#show bandwidth_control 1-5
Command: show bandwidth_control 1-5

Bandwidth Control Table

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

DES-3028P:4#
```

config scheduling

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

Example usage:

To configure the traffic scheduling mechanism for each queue:

```
DES-3028P:4# config scheduling 0 weight 55
Command: config scheduling 0 weight 55

Success.

DES-3028P:4#
```

show scheduling

Purpose	Used to display the currently configured traffic scheduling on the Switch.
Syntax	**show scheduling**
Description	The **show scheduling** command will display the current traffic scheduling mechanisms in use on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```
DES-3028P:4# show scheduling
Command: show scheduling

QOS Output Scheduling

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

DES-3028P:4#
```

config scheduling_mechanism

Purpose	Used to configure the scheduling mechanism for the QoS function
Syntax	**config scheduling_mechanism [strict | weight_fair]**
Description	The **config scheduling_mechanism** command allows the user to select between a **weight fair** and a **Strict** mechanism for emptying the priority classes of service of the QoS function. The Switch contains seven hardware priority classes of service. Incoming packets must be mapped to one of these seven hardware priority classes of service. This command is used to specify the rotation by which these seven hardware priority classes of service are emptied. The Switch's default is to empty the seven priority classes of service in order – from the highest priority class of service (queue 6) to the lowest priority class of service (queue 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority class of service to transmit its packets. Lower classes of service will be pre-empted from emptying its queue if a packet is received on a higher class of service. The packet that was received on the higher class of service will transmit its packet before allowing the lower class to resume clearing its queue.
Parameters	*strict* – Entering the *strict* parameter indicates that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin. *weight_fair* – Entering the weight fair parameter indicates that the priority classes of service will empty packets in a fair weighted order. That is to say that they will be emptied in an even distribution.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each QoS queue:

```
DES-3028P:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Note: The strict mode is only supported at the highest
queue
and the other lower queues will still work at WRR mode.

Success.

DES-3028P:4#
```

show scheduling_mechanism

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

Example usage:

To show the scheduling mechanism:

```
DES-3028P:4#show scheduling_mechanism
Command: show scheduling_mechanism

QOS scheduling_mechanism
CLASS ID    Mechanism
--------    -----------
Class-0        strict
Class-1        strict
Class-2        strict
Class-3        strict

DES-3028P:4#
```

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

Example usage:

To configure 802.1p user priority on the Switch:

```
DES-3028P:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-3028P:4#
```

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

Example usage:

To show 802.1p user priority:

```
DES-3028P:4# show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

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

DES-3028P:4#
```

config 802.1p default_priority

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

Example usage:

To configure 802.1p default priority on the Switch:

```
DES-3028P:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3028P:4#
```

show 802.1p default_priority

Purpose	Used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Syntax	**show 802.1p default_priority {<portlist>}**
Description	The **show 802.1p default_priority** command displays the currently

show 802.1p default_priority	
	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-3028P:4# show 802.1p default_priority
Command: show 802.1p default_priority

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

DES-3028P:4#
```

config cos mapping

Purpose	Used to configure the CoS to port mapping method to be used on the switch.
Syntax	**config cos mapping port [<portlist> | all] [none | {port_mapping | ethernet [802.1p | mac_mapping] | ip [tos | dscp]}]**
Description	The **config cos mapping** is used to set the method of which incoming packets will be identified for the CoS to port mapping feature on the Switch. Identified packets will be forwarded to the appropriate CoS queue.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *all* – Specifies all ports will be configured. *none* – Disable all priority-base CoS features. *port_mapping* – Enable port-based CoS. *ethernet* – Enable Ethernet frame based priority. *802.1p* – Enable 802.1p CoS *mac_mapping* – Enable MAC-based CoS. *ip* – Enable Ethernet frame based priority.
Restrictions	None.

Example usage:

To configure port 1 as a CoS enabled port which uses the physical port number as its criteria for identifying packets:

```
DES-3028P:4#config   cos   mapping   port   1
port_mapping
Command:   config   cos   mapping   port   1
port_mapping

Success.

DES-3028P:4#
```

show cos mapping

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

Example usage:

To show the CoS mapping information:

```
DES-3028P:4# show cos mapping
Command: show cos mapping

Port     Port_priority       Ethernet_priority          IP_priority
----------------------------------------------------------------------
1               off             802.1p                          off
2               off             802.1p                          off
```

```
3               off             802.1p                          off
4               off             802.1p                          off
5               off             802.1p                          off
6               off             802.1p                          off
7               off             802.1p                          off
8               off             802.1p                          off
9               off             802.1p                          off
10              off             802.1p                          off
11              off             802.1p                          off
12              off             802.1p                          off
13              off             802.1p                          off
14              off             802.1p                          off
15              off             802.1p                          off
16              off             802.1p                          off
17              off             802.1p                          off
18              off             802.1p                          off
19              off             802.1p                          off
20              off             802.1p                          off
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config cos port_mapping

Purpose	Used to map a specific port to one of the hardware queues available on the switch.
Syntax	**config cos port_mapping [0-3] port [<portlist> | all]**
Description	The config cos port_mapping command is used to configure port-to-class CoS mapping.
Parameters	*0-3* – The number of the switch’s hardware priority queue. The switch has eight hardware priority queues available. They are numbered between 0 (the lowest priority queue) and 3 (the highest priority queue). *<portlist>* – Specifies a port or range of ports to be configured. *all* – To set all ports in the system at once, you may use the “all” parameter.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a specific CoS queue to be mapped to a destination port 1:

```
DES-3028P:4# config cos port_mapping 3 port 1
Command: config cos port_mapping 3 port 1

Success.

DES-3028P:4#
```

show cos port_mapping

Purpose	Used to map the destination MAC address in incoming packets to one of the hardware queues available on the switch.
Syntax	**show cos port_mapping {port <portlist>}**
Description	The **show cos mac_mapping** command is used to view map static destination MAC addresses to one of the CoS traffic classes.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. If no parameter is specified, all port-to-class mappings will be shown.
Restrictions	None.

Example usage:

To show the cos port_mapping of the port 3:

```
DES-3028P:4# show cos port_mapping port 3
Command: show cos port_mapping port 3

Port  Priority
------------------
 3       3

DES-3028P:4#
```

config cos mac_mapping

Purpose	Used to map the destination MAC address in incoming packet to one of the hardware queues available on the switch.
Syntax	**config cos mac_mapping destination_addr <macaddr> [class <class_id 0-3>]**
Description	The **config cos mac_mapping** command is used to map static destination MAC address to one of the traffic classes.
Parameters	*destination_addr* – The MAC address to be configured. *<class_id 0-3>* – The number of the Switch's hardware priority queue. The Switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the destination MAC address 00-01-02-03-04-05 to traffic class 2 mapping:

```
DES-3028P:4# config cos mac_mapping destination_addr 00-01-02-03-
04-05 class 2
Command: config cos mac_mapping destination_addr 00-01-02-03-04-
05 class 2


Success.


DES-3028P:4#
```

show cos mac_mapping

Purpose	Used to show the mapping between destination MAC addresses and CoS traffic classes.
Syntax	**show cos mac_mapping {destination_addr <macaddr>}**
Description	The **show cos mac_mapping** command display the information of the destination MAC address mapped to a traffic class.
Parameters	*destination_addr* – The MAC address of the incoming packet destination address. If no parameter is specified, all the MAC address mapping to traffic class will be shown.
Restrictions	None.

Example usage:

To show the MAC address to traffic class mapping of MAC address 00-01-02-03-04-05:

```
DES-3028P:4# show cos mac_mapping destination_addr 00-01-
02-03-04-05
Command: show cos mac_mapping destination_addr  00-01-02-
03-04-05

MAC Address             Class
---------------------------------------
00-01-02-03-04-05        2

DES-3028P:4#
```

config cos tos value

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

Example usage:

Configure the TOS 5 to the traffic class 1 mapping:

```
DES-3028P:4# config cos tos value 5 class 1
Command: config cos tos value 5 class 1

Success.

DES-3028P:4#
```

show cos tos

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

Example usage:

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

```
DES-3028P:4# show cos tos value 5
Command: show cos tos value 5

TOS value             Class
-------------------------------------------
5                             2

DES-3028P:4#
```

config dscp_mapping

Purpose	Used to map the DSCP value in the IP header of incoming packet to one of the four hardware queues available on the switch.
Syntax	**config dscp_mapping dscp_value <value 0-63> [class <class_id 0-3>]**
Description	The **config dscp_mapping** command is used to configure DSCP mapping to traffic class. This command is supported when the ACL commands are not supported.
Parameters	*<value 0-63>* – The DSCP value of the incoming packet you want to associate with the class_id. *<class_id 0-3>* – The number of the Switch's hardware priority queue. The switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DSCP map to traffic class:

```
DES-3028P:4# config dscp_mapping dscp_value 8 
class 1
Command: config dscp_mapping dscp_value 8 
class 1

Success.

DES-3028P:4#
```

show dscp_mapping

Purpose	Used to show DSCP value map to traffic class.
Syntax	**show dscp_mapping {dscp_value <value 0-63>}**
Description	The **show dscp_mapping** command displays the information for DSCP mapping to traffic class. This command is supported when the ACL commands are not supported.
Parameters	*<value 0-63>* – The DSCP value of the incoming packet. If no parameter is specified, all the DSCP value mapping to traffic class will be shown.
Restrictions	None.

Example usage:

To show the DSCP map to traffic class:

```
DES-3028P:4# show dscp_mapping
Command: show dscp_mapping

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

15

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	*<port>* – 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. *[add | delete]* – Specifies if the user wishes to add or delete ports to be mirrored that are specified in the *source ports* parameter. *source ports* – The port or ports being mirrored. This cannot include the Target port. *<portlist>* – This specifies a port or range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port. *rx* – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list. *tx* – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list. *both* – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	The Target port cannot be listed as a source port. Only Administrator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DES-3028P:4# config mirror port 1 add source ports 2-7
both
```

```
Command: config mirror port 1 add source ports 2-7 both

Success.

DES-3028P:4#
```

Example usage:

To delete the mirroring ports:

```
DES-3028P:4#config mirror port 1 delete source port 2-4
both
Command: config mirror 1 delete source 2-4 both

Success.

DES-3028P:4#
```

enable mirror

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

Example usage:

To enable mirroring configurations:

```
DES-3028P:4#enable mirror
Command: enable mirror

Success.

DES-3028P:4#
```

disable mirror

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

Example usage:

To disable mirroring configurations:

```
DES-3028P:4#disable mirror
```

```
Command: disable mirror

Success.

DES-3028P:4#
```

show mirror

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

Example usage:

To display mirroring configuration:

```
DES-3028P:4#show mirror
Command: show mirror

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

DES-3028P:4#
```

16

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

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

create vlan

Purpose	Used to create a VLAN on the Switch.
Syntax	**create vlan <vlan_name 32> {tag <vlanid 2-4094> | advertisement}**
Description	This command allows the user to create a VLAN on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN to be created. *<vlanid 2-4094>* – The VLAN ID of the VLAN to be created. Allowed values = 2-4094 *advertisement* – Specifies that the VLAN is able to join GVRP. If this parameter is not set, the VLAN cannot be configured to have forbidden ports.
Restrictions	Each VLAN name can be up to 32 characters. Up to 4094 static VLANs may be created per configuration. Only Administrator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DES-3028P:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.
```

```
DES-3028P:4#
```

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 delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To remove the VLAN “v1”:

```
DES-3028P:4#delete vlan v1
Command: delete vlan v1

Success.

DES-3028P:4#
```

config vlan

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

Example usage:

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

```
DES-3028P:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DES-3028P:4#
```

To delete ports from a VLAN:

```
DES-3028P:4#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.

DES-3028P:4#
```

create vlan vlanid

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

Example usage:

To create VLAN ID on the switch:

```
DES-3028P:4#create vlan vlanid 5 advertisement
Command: create vlan vlanid 5 advertisement

Success

DES-3028P:4#
```

delete vlan vlanid

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

Example usage:

To delete VLAN ID on the switch:

```
DES-3028P:4#delete vlan vlanid 5
Command: delete vlan vlanid 5

Success

DES-3028P:4#
```

config vlan vlanid

Purpose	Used to add additional ports to a previously configured VLAN.

config vlan vlanid	
Syntax	**config vlan vlanid <vidlist> {add [tagged | untagged | forbidden] | delete <portlist> | advertisement [enable | disable] | name <name>}**
Description	The config vlan vlanid 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 ports will join GVRP or not with the *advertisement* parameter. The *name* parameter allows you to specify the name of the VLAN that needs to be modified.
Parameters	<*vidlist*> – Specifies a range of multiple VLAN IDs to be configured. *tagged* – Specifies the additional ports as tagged. *untagged* – Specifies the additional ports as untagged. *forbidden* – Specifies the additional ports as forbidden. <*portlist*> – A range of ports to add to the VLAN. *advertisement* – Entering the advertisement parameter specifies if the port should join GVRP or not. There are two parameters: ▪ *enable* – Specifies that the port should join GVRP. ▪ *Disable* – Specifies that the port should not join GVRP. *name* – Entering the name parameter specifies the name of the VLAN to be modified. <*name*> – Enter a name for the VLAN
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config vlan vlanid on the switch:

```
DES-3028P:4#config vlan vlanid 5 add tagged 7
advertisement enable name RG
Command: config vlan vlanid 5 add tagged 7 advertisement
enable name RG

Success.

DES-3028P:4#
```

config gvrp	
Purpose	Used to configure GVRP on the Switch.
Syntax	**config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}**
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	<*portlist*> – A port or range of ports for which users want to enable GVRP for. *all* – Specifies all of the ports on the Switch. *state [enable* | *disable]* – Enables or disables GVRP for the ports specified in the port list.

config gvrp	
	ingress_checking [enable | *disable]* – Enables or disables ingress checking for the specified port list. *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. *pvid <vlanid 1-4094>* – Specifies the default VLAN associated with the port.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#config gvrp 1-4 state enable ingress_checking
enable acceptable_frame tagged_only pvid 2
Command:  config  gvrp  1-4  state  enable  ingress_checking
enable acceptable_frame tagged_only pvid 2


Success.


DES-3028P:4#
```

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

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DES-3028P:4#enable gvrp
Command: enable gvrp

Success.

DES-3028P:4#
```

disable gvrp	
Purpose	Used to disable GVRP on the Switch.
Syntax	**disable gvrp**
Description	This command, along with **enable gvrp**, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.

disable gvrp

Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DES-3028P:4#disable gvrp
Command: disable gvrp

Success.

DES-3028P:4#
```

show vlan

Purpose	Used to display the current VLAN configuration on the Switch
Syntax	**show vlan [<vlan_name 32> | vlanid <vidlist> | ports <portlist>]**
Description	This command displays summary information about each VLAN including the VLAN ID, VLAN name, VLAN Type, the Tagging/Untagging status, and the Member/Non-member/Forbidden status of each port that is a member of the VLAN.
Parameters	*<vlanid>* – Specifies a range of multiple VLAN IDs to be displayed. *<ports>* – Specifies the ports to be displayed. *<vlan_name 32>* – The VLAN name of the VLAN for which to display a summary of settings. *<portlist>* – Specifies a port or range of ports that will be displayed.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DES-3028P:4#show vlan
Command: show vlan
VID             : 1          VLAN Name       : default
VLAN Type       : Static     Advertisement   : Enabled
Member Ports    : 1-28
Static Ports    : 1-28
Current Tagged Ports   :
Current Untagged Ports : 1-28
Static Tagged Ports    :
Static Untagged Ports  : 1-28
Forbidden Ports        :


Total Entries  : 1

DES-3028P:4#
```

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

```
DES-3028P:4# DES-3028P:4#show vlan port 1
Command: show vlan ports 1

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

DES-3028P:4#
```

show gvrp

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

Example usage:

To display GVRP port status:

```
DES-3028P:4#show gvrp 1-10
Command: show gvrp 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
```

17

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 1-6> {type [lacp | static]}
delete link_aggregation	group_id <value 1-6>
config link_aggregation	group_id <value 1-6> {master_port <port> | ports <portlist> | state [enable | disable]}
config link_aggregation algorithm	[mac_source | mac_destination | mac_source_dest]
show link_aggregation	{group_id <value 1-6> | 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 1-6> {type[lacp | static]}**
Description	This command will create a link aggregation group with a unique identifier.
Parameters	*<value>* – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *type* – Specify the type of link aggregation used for the group. If the type is not specified the default type is *static*. • *lacp* – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices. • *static* – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunk group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DES-3028P:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.
DES-3028P:4#
```

delete link_aggregation group_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value 1-6>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	*<value 1-6>* – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DES-3028P:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DES-3028P:4#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-6> {master_port <port> | ports <portlist> | state [enable | disable]**
Description	This command allows users to configure a link aggregation group that was created with the **create link_aggregation** command above.
Parameters	*group _id <value 1-6>* – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *master_port <port>* – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. *ports <portlist>* – Specifies a port or range of ports that will belong to the link aggregation group. *state [enable | disable]* – Allows users to enable or disable the specified link aggregation group.
Restrictions	Only Administrator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

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

```
DES-3028P:4#config link_aggregation group_id 1 master_port
1 ports 1-4
Command: config link_aggregation group_id 1 master_port 1
ports 1-4

Success.

DES-3028P:4#
```

config link_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
Syntax	**config link_aggregation algorithm [mac_source | mac_destination | mac_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	*mac_source* – Indicates that the Switch should examine the MAC source address. *mac_destination* – Indicates that the Switch should examine the MAC destination address. *mac_source_dest* – Indicates that the Switch should examine the MAC source and destination addresses
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4#config      link_aggregation      algorithm
mac_source_dest
Command:     config     link_aggregation     algorithm
mac_source_dest

Success.

DES-3028P:4#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the Switch.
Syntax	**show link_aggregation {group_id <value 1-6> | algorithm}**
Description	This command will display the current link aggregation configuration of the Switch.
Parameters	*<value 1-6>* – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *algorithm* – Allows users to specify the display of link aggregation by the algorithm in use by that group.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DES-3028P:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest

Group ID         : 1
Master Port      : 1
Member Port      : 1, 5-10
Active Port      :
Status           : Disabled
Flooding Port    : 0

DES-3028P:4#
```

config lacp_ports

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

Example usage:

To configure LACP port mode settings:

```
DES-3028P:4#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DES-3028P:4#
```

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	Only Administrator-level users can issue this command.

Example usage:

To display LACP port mode settings:

```
DES-3028P:4#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-3028P:4#
```

18

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	[System] [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp]
show ipif	
enable autoconfig*	

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

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

config ipif

Purpose	Used to configure the System IP interface.
Syntax	**config ipif [System] [{ipaddress <network_address> [vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp]**
Description	This command is used to configure the System IP interface on the Switch.
Parameters	*System* – Enter System. *ipaddress <network_address>* – IP address and netmask of the IP interface to be created. Users can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format 10.1.2.3/8). *<vlan_name 32>* – The name of the VLAN corresponding to the System IP interface. *state [enable | disable]* – Allows users to enable or disable the IP interface. *bootp* – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface. *dhcp* – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System 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.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DES-3028P:4#config ipif System ipaddress
10.48.74.122/8
Command: config ipif System ipaddress
10.48.74.122/8

Success.

DES-3028P:4#
```

show ipif

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

Example usage:

To display IP interface settings.

```
DES-3028P:4#show ipif
Command: show ipif

IP Interface Settings

Interface Name  : System
IP Address      : 10.48.74.122    (MANUAL)
Subnet Mask     : 255.0.0.0
VLAN Name       : default
Admin. State    : Disabled
Link Status     : Link UP
Member Ports    : 1-28

Total Entries : 1

DES-3028P:4#
```

enable autoconfig

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

Example usage:

To enable auto configuration on the Switch:

```
DES-3028P:4#enable autoconfig
Command: enable autoconfig

Success.

DES-3028P:4#
```

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

19

IGMP SNOOPING COMMANDS

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

Command	Parameters
config igmp_snooping	[vlan_name <vlan_name 32> |all] { host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state [enable|disable] | fast_leave [enable|disable]}
config igmp_snooping querier	[vlan_name <vlan_name 32> | 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]}
config router_ports	<vlan_name 32> [add | delete] <portlist>
config router_port_forbidden	<vlan_name 32> [add | delete] <portlist>
enable igmp snooping	{forward_mcrouter_only}
show igmp snooping	{vlan <vlan_name 32> }
disable igmp snooping	{forward_mcrouter_only}
show router ports	{vlan <vlan_name 32>} {[static | dynamic | forbidden]}
show igmp_snooping group	{vlan <vlan_name 32>} {data_driven}
config igmp snooping data_driven_learning	[vlan_name <vlan_name 32> |all] { aged_out [enable|disable]}
config igmp_snooping data_driven_learning max_learned_entry	<value 1-256>
clear igmp snooping data_ driven _group	[vlan_name <vlan_name 32> | all]
config igmp access_authentication	ports [all|<portlist>] state [enable|disable]
show igmp access_authentication	ports [all|<portlist>]

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

config igmp_snooping

Purpose	Used to configure IGMP snooping on the Switch.
Syntax	**[vlan_name <vlan_name 32> |all] { host_timeout <sec 1-16711450> | route r_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state [enable|disable] | fast_leave [enable|disable]}**
Description	This command allows the user to configure IGMP snooping on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping is to be configured. *host_timeout <sec 1-16711450>* – Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. *router_timeout <sec 1-16711450>* – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds.

config igmp_snooping

	leave_timer <sec 0-16711450> – Specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted. The default setting is 2. Note: The leave timer does not need to be configured as its action has no effect on the IGMP snooping settings. *state [enable* | *disable]* – Allows users to enable or disable IGMP snooping for the specified VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-3028P:4# config igmp_snooping default host_timeout 250
state enable
Command: config igmp_snooping default host_timeout 250 state
enable

Success.

DES-3028P:4#
```

config igmp_snooping querier

Purpose	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping.
Syntax	**config igmp_snooping querier [vlan <vlan_name 32> | 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] }**
Description	The **config igmp_snooping querier** command configures IGMP snooping querier.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping querier is to be configured. *query_interval <sec 1-25>* – Specifies the amount of time in seconds between general query transmissions. the default setting is *125* seconds. *max_response_time* – The maximum time in seconds to wait for reports from members. The default setting is *10* seconds. *robustness_variable* – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: • Group 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.

config igmp_snooping querier	
	• By default, the robustness variable is set to *2*. You might want to increase this value if you expect a subnet to be lossy. *last_member_query_interval* – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. *state* – If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). It the state is disabled, then the switch can not play the role as a querier. Note that if the Layer 3 router connected to the switch provide only the IGMP proxy function but not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure IGMP snooping querier:

```
DES-3028P:4# 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-3028P:4#
```

config router_ports	
Purpose	Used to configure ports as router ports.
Syntax	**config router_ports <vlan_name 32> [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	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *<portlist>* – Specifies a port or range of ports that will be configured as router ports.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set up static router ports:

```
DES-3028P:4#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DES-3028P:4#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden multicast router ports.
Syntax	**config router_ports_forbidden <vlan_name 32> [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	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *[add | delete]* – Specifies whether to add or delete forbidden ports of the specified VLAN. *<portlist>* – Specifies a range of ports that will be configured as forbidden router ports.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set up forbidden router ports:

```
DES-3028P:4# config router_ports_forbidden default add
2-10
Command: config router_ports_forbidden default add 2-10

Success.

DES-3028P:4#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**enable igmp_snooping {forward_mcrouter_only}**
Description	This command allows users to enable IGMP snooping on the Switch. If *forward_mcrouter_only* is specified, the Switch will only forward all multicast traffic to the multicast router, only. Otherwise, the Switch forwards all multicast traffic to any IP router.
Parameters	*forward_mcrouter_only* – Specifies that the Switch should only forward all multicast traffic to a multicast-enabled router. Otherwise, the Switch will forward all multicast traffic to any IP router.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DES-3028P:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3028P:4#
```

disable igmp_snooping	
Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**disable igmp_snooping {forward_mcrouter_only}**
Description	This command disables IGMP snooping on the Switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.
Parameters	*forward_mcrouter_only* – Adding this parameter to this command will disable forwarding all multicast traffic to a multicast-enabled routers. The Switch will then forward all multicast traffic to any IP router. Entering this command without the parameter will disable igmp snooping on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DES-3028P:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3028P:4#
```

Example usage:

To disable forwarding all multicast traffic to a multicast-enabled router:

```
DES-3028P:4#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only

Success.

DES-3028P:4#
```

show igmp_snooping	
Purpose	Used to show the current status of IGMP snooping on the Switch.
Syntax	**show igmp_snooping {vlan <vlan_name 32>}**
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.
Restrictions	None.

Example usage:

To show IGMP snooping:

```
DES-3028P:4#show igmp_snooping
Command: show igmp_snooping

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

 VLAN  Name                    : default
 Query Interval                : 125
 Max Response Time             : 10
 Robustness Value              : 2
 Last Member Query Interval    : 1
 Host Timeout                  : 260
 Route Timeout                 : 260
 Leave Timer                   : 2
 Querier State                 : Disabled
 Querier Router Behavior       : Non-Querier
 State                         : Disabled
 Multicast Fast Leave          : Disabled
 Data Driven Learning Aged Out : Disabled


 VLAN  Name                    : RG
 Query Interval                : 125
 Max Response Time             : 10

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

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

Example usage:

To display the router ports.

```
DES-3028P:4#show router_ports
Command: show router_ports

VLAN Name              : default
Static router port     : 1-2,10
Dynamic router port    :


Total Entries: 1

DES-3028P:4#
```

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>} {data_driven}**
Description	This command will display the current IGMP setup currently configured on the Switch.
Parameters	<*vlan_name 32*> – The name of the VLAN for which to view IGMP snooping group information. *data_driven* – hen the data driven learning is enabled, the multicast filtering mode for all ports are ignored.
Restrictions	None.

Example usage:

To view the current IGMP snooping group:

```
DES-3028P:4#show igmp_snooping group
Command: show igmp_snooping group

VLAN Name          : default
Multicast group    : 224.0.0.2
MAC address        : 01-00-5E-00-00-02
Reports            : 1
Port Member        : 2,4

VLAN Name          : default
Multicast group    : 224.0.0.9
MAC address        : 01-00-5E-00-00-09
Reports            : 1
Port Member        : 6,8

VLAN Name          : default
Multicast group    : 234.5.6.7
MAC address        : 01-00-5E-05-06-07
Reports            : 1
Port Member        : 10,12

VLAN Name          : default
Multicast group    : 236.54.63.75
MAC address        : 01-00-5E-36-3F-4B
Reports            : 1
Port Member        : 14,16

VLAN Name          : default
Multicast group    : 239.255.255.250
MAC address        : 01-00-5E-7F-FF-FA
Reports            : 2
Port Member        : 18,20

VLAN Name          : default
Multicast group    : 239.255.255.254
MAC address        : 01-00-5E-7F-FF-FE
Reports            : 1
Port Member        : 22,24

Total Entries : 6

DES-3028P:4#
```

config igmp snooping data_driven_learning

Purpose	Used to configure the data driven learning of a IGMP snooping group.
Syntax	**[vlan_name <vlan_name 32> |all] { aged_out [enable|disable]}**
Description	This command is used to enable/disable the data driven learning of a IGMP snooping group. When data-driven learning is enabled for the VLAN, or when the switch receives the IP multicast traffic on this VLAN, an IGMP snooping group will be created. The learning of an entry is not activated by IGMP membership registration, but by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will acknowledge the aging out of the entry. For a data-driven entry, the entry can be specified so that it won't be ageout or that it will be ageout by the host_timeout timer. When the data driven learning is enabled, the multicast filtering mode for all ports are ignored so that the multicast packets will be forwarded to router ports. Note that if a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. The ageing out mechanism will follow the ordinary IGMP snooping entry.
Parameters	*<vlan_name 32>* – specifies the vlan name to be configured. *all* – specifies all data driven entries. *aged_out* – Used to enable/disable the aging on the entry. By default, the state is in disabled state.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the igmp snooping data driven entry:

```
DES-3028P:4#config igmp_snooping
data_driven_learning vlan_name default aged_out
enable
Command: config igmp_snooping data_driven_learning
vlan_name default aged_out enable

Success.

DES-3028P:4#
```

config igmp_snooping data_driven_learning max_learned_entry

Purpose	Used to configure the IGMP snooping data driven learning max learned entry.
Syntax	**<value 1-256>**
Description	Used to configure the IGMP snooping data driven learning max learned entry.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure igmp_snooping data_driven_learning max_learned_entry:

```
DES-3028P:4#         config         igmp_snooping
data_driven_learning max_learned_entry 1
Command: config igmp_snooping data_driven_learning
max_learned_entry 1

Success.

DES-3028P:4#
```

clear igmp snooping data_driven_group

Purpose	Used to delete the IGMP snooping group learned by data driven.
Syntax	**[vlan_name <vlan_name 32> [all | <ipaddr>] | all]**
Description	Used to delete the IGMP snooping group learned by data driven. Note that this command is currently only for layer 2 switches.
Parameters	*all* – Delete all entries learned by data driven. <*vlan_name 32*> – Specifies the vlan name. <*ipaddr*> – Specifies the IP Address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete all the groups learned by data-driven :

```
DES-3028P:4# clear igmp snooping data_driven_group
all
Command: clear igmp snooping data_driven_group all

Success.

DES-3028P:4#
```

config igmp access_authentication

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

Example usage:

To enable IGMP Access Control for all ports :

```
DES-3028P:4#   config   igmp   access_authentication
ports all state enable
Command:  config  igmp  access_authentication  ports
all state enable

Success.

DES-3028P:4#
```

show igmp access_authentication

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

Example usage:

To display IGMP Access Control status for all ports :

```
DES-3028P:4# show igmp access_authentication ports
1-4
Command: show igmp access_authentication ports 1-4

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

DES-3028P:4#
```

20

DHCP RELAY

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>}
config dhcp_relay add ipif System	<ipaddr>
config dhcp_relay delete ipif System	<ipaddr>
config dhcp_relay option_82 state	[enable | disable]
config dhcp_relay option_82 check	[enable | disable]
config dhcp_relay option_82 policy	[replace | drop | keep]
config dhcp_relay option_82 remote_id	[default | user_define <string 32>]
show dhcp_relay	{ipif [System]}
enable dhcp_relay	
disable dhcp_relay	

Each command is listed in detail in the following sections.

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

Example usage:

To config DHCP relay:

```
DES-3028P:4#config dhcp_relay hops 2 time 23
Command: config dhcp_relay hops 2 time 23

Success.

DES-3028P:4#
```

config dhcp_relay add ipif	
Purpose	Used to add an IP destination address to the switch's DHCP/BOOTP relay table.
Syntax	**config dhcp_relay add ipif System <ipaddr>**
Description	This command adds an IP address as a destination to forward (relay) DHCP/BOOTP relay packets to.
Parameters	*System* – The name of the IP interface in which DHCP relay is to be enabled.

config dhcp_relay add ipif

	<ipaddr> – The DHCP server IP address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add an IP destination to the DHCP relay table:

```
DES-3028P:4#config dhcp_relay add ipif System
10.58.44.6
Command: config dhcp_relay add ipif System
10.58.44.6

Success.

DES-3028P:4#
```

config dhcp_relay delete ipif

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

Example usage:

To delete an IP destination from the DHCP relay table:

```
DES-3028P:4#config dhcp_relay delete ipif System
10.58.44.6
Command: config dhcp_relay delete ipif System
10.58.44.6

Success.

DES-3028P:4#
```

config dhcp_relay option_82 state

Purpose	Used to configure the state of DHCP relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 state [enable | disable]**
Description	This command is used to configure the state of DHCP relay agent information option 82 of the switch.
Parameters	*enable* – When this field is toggled to *Enabled* the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP server and client. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like

config dhcp_relay option_82 state

	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. *disable* – If the field is toggled to *disable* the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DES-3028P:4#config dhcp_relay option_82 state
enable
Command: config dhcp_relay option_82 state
enable


Success.


DES-3028P:4#
```

config dhcp_relay option_82 check

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

Example usage:

To configure DHCP relay option 82 check:

```
DES-3028P:4#config dhcp_relay option_82 check
enable
Command: config dhcp_relay option_82 check
enable


Success.


DES-3028P:4#
```

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	*replace* – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *drop* – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *keep* – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 policy:

```
DES-3028P:4#config dhcp_relay option_82 policy
replace
Command: config dhcp_relay option_82 policy
replace

Success.

DES-3028P:4#
```

config dhcp_relay option_82 remote id

Purpose

Used to configure the processing of DHCP 82 remote id option for the DHCP.

Syntax

config dhcp_relay option_82 remote_id [default | user_define <string 32>]

Description

Configures the processing of DHCP 82 option for the DHCP relay function.

When DHCP 82 option is enabled, the DHCP packet received from the client will be inserted with option 82 field before being relayed to the server. The DHCP 82 option contained 2 suboptions which is circuit ID suboption and remote ID suboption.

The formats for the circuit ID suboption and the remote ID suboption are as following. For the circuit ID suboption of a standalone switch, the module field is always zero.

Remote ID suboption format 2 (Using user-defined string as remote ID):

1.	2.	3.	4.	5.
2	n + 2	1	n	User-defined string
1 byte	1 byte	1 byte	1 byte	6 bytes

1. Suboption type 2. Length : the string length of Remote ID suboption

3. Remote ID type 4. Length : the string length of user-defined string

5. User-defined string

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 remote id :

```
DES-3028P:4#config dhcp_relay option_82
remote_id user_define “D-Link L2 Switch”
Command: config dhcp_relay option_82 remote_id
user_define "D-Link L2 Switch”


DES-3028P:4#
```

show dhcp_relay

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

Example usage:

To show the DHCP relay configuration:

```
DES-3028P:4#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status         : Disabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State     : Disabled
DHCP Relay Agent Information Option 82 Check     : Disabled
DHCP Relay Agent Information Option 82 Policy    : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-19-5B-EF-78-B5

Interface     Server 1         Server 2         Server 3         Server 4
-----------  --------------  --------------  --------------  -------------

DES-3028P:4#
```

Example usage:

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

```
DES-3028P:4#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

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

DES-3028P:4#
```

enable dhcp_relay

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

Example usage:

To enable DHCP relay:

```
DES-3028P:4#enable dhcp_relay
Command: enable dhcp_relay

Success.

DES-3028P:4#
```

disable dhcp_relay

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

Example usage:

To disable DHCP relay:

```
DES-3028P:4#disable dhcp_relay
Command: disable dhcp_relay

Success.

DES-3028P:4#
```

21

802.1X COMMANDS

The DES-3028/28G/28P/52/52P implements IEEE 802.1X Port-based and Host-based Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames.

Command	Parameters
enable 802.1x	
disable 802.1x	
show 802.1x auth_state	{ports <auth_portlist>}
show 802.1x auth_configuration	{ports <auth_portlist>}
config 802.1x capability ports	[<auth_portlist> | all] [authenticator | none]
config 802.1x auth_parameter ports	[<auth_portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]
config 802.1x auth_protocol	[radius_eap | local]
config 802.1x init	{port_based ports [<auth_portlist> | all] | mac_based [ports] [<auth_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>}]
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>]}
config radius parameter	{ timeout <int 1-255> | retransmit <int 1-255>}
show radius	
create 802.1x guest_vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> | all] state [enable | disable]
delete 802.1x guest_vlan	{<vlan_name 32>}
show 802.1x guest_vlan	
show auth_statistics	{ports <auth_portlist>}
show auth_diagnostics	{ports <auth_portlist>}
show auth_session_statistics	{ports <auth_portlist>}
show auth_client	
show acct_client	
create 802.1x user	<username 15>
delete 802.1x user	<username 15>
show 802.1x user	

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

enable 802.1x

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

Example usage:

To enable 802.1X switch wide:

```
DES-3028P:4#enable 802.1x
Command: enable 802.1x

Success.

DES-3028P:4#
```

disable 802.1x

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

Example usage:

To disable 802.1x on the Switch:

```
DES-3028P:4#disable 802.1x
Command: disable 802.1x

Success.

DES-3028P:4#
```

show 802.1x auth_configuration	
Purpose	Used to display the current configuration of the 802.1X server on the Switch.
Syntax	**show 802.1x auth_configuration {ports <auth_portlist>}**
Description	The **show 802.1x auth_configuration** command is used to display the 802.1X Port-based or Host-based Network Access control local users currently configured on the Switch.
Parameters	*ports <auth_portlist>* – Specifies a port or range of ports to view. The following details are displayed: *802.1x Enabled / Disabled* – Shows the current status of 802.1X functions on the Switch. *Authentication Mode* – Shows the authentication mode, whether it be by MAC address or by port. *Authentication Protocol* – Shows the authentication protocol suite in use between the Switch and a RADIUS server. May read *Radius_Eap* or *local.* *Port number* – Shows the physical port number on the Switch. Capability: Authenticator/None – Shows the capability of 802.1X functions on the port number displayed above. There are two 802.1X capabilities that can be set on the Switch: Authenticator and None. *AdminCtlDir: Both / In* – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. *OpenCtlDir: Both / In* – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. *Port Control: ForceAuth / ForceUnauth / Auto* – Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized. *QuietPeriod* – This is the initialization value of the quiet period timer. The default value is 60s and can be any value between 0-65535. *TxPeriod* – This us the initialization value of the tx timer. The default value is 30s and can be any value between 1-65535. *SuppTimeout* – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request / Identity packets. *ServerTimeout* – Shows the length of time to wait for a response from a RADIUS server. *MaxReq* – Shows the maximum number of times to retry sending packets to the supplicant. *ReAuthPeriod* – Shows the time interval between successive re-authentications. *ReAuthenticate: Enabled / Disabled* – Shows whether or not to re-authenticate.
Restrictions	None.

Example usage:

To display the 802.1X authentication states:

```
DES-3028P:4#show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

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

Port number          : 1
Capability           : None
AdminCrlDir          : Both
OpenCrlDir           : Both
Port Control         : Auto
QuietPeriod          : 60 sec
TxPeriod             : 30 sec
SuppTimeout          : 30 sec
ServerTimeout        : 30 sec
MaxReq               : 2 times
ReAuthPeriod         : 3600 sec
ReAuthenticate       : Disabled

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

show 802.1x auth_state

Purpose	Used to display the current authentication state of the 802.1X server on the Switch.
Syntax	**show 802.1x auth_state {ports <auth_portlist>}**
Description	The **show 802.1x auth_state** command is used to display the current authentication state of the 802.1X Port-based or Host-based Network Access Control application on the Switch.
Parameters	*<auth_portlist>* – Specifies a port or range of ports to be viewed. The following details what is displayed: Port number – Shows the physical port number on the Switch. Auth PAE State: Initalize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE. Backend State: Request / Response / Fail / Idle / Initalize / Success / Timeout – Shows the current state of the Backend Authenticator. Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Restrictions	None.

Example usage:

To display the 802.1X auth state for Port-based 802.1X:

```
DES-3028P:4#show 802.1x auth_state
Command: show 802.1x auth_state

Port         Auth PAE State         Backend State        Port Status
------      -----------------      -----------------     -----------------
1               ForceAuth              Success            Authorized
2               ForceAuth              Success            Authorized
3               ForceAuth              Success            Authorized
4               ForceAuth              Success            Authorized
5               ForceAuth              Success            Authorized
6               ForceAuth              Success            Authorized
7               ForceAuth              Success            Authorized
8               ForceAuth              Success            Authorized
9               ForceAuth              Success            Authorized
10              ForceAuth              Success            Authorized
11              ForceAuth              Success            Authorized
12              ForceAuth              Success            Authorized
13              ForceAuth              Success            Authorized
14              ForceAuth              Success            Authorized
15              ForceAuth              Success            Authorized
16              ForceAuth              Success            Authorized
17              ForceAuth              Success            Authorized
18              ForceAuth              Success            Authorized
19              ForceAuth              Success            Authorized
20              ForceAuth              Success            Authorized

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

Example usage:

To display the 802.1X auth state for Host-based 802.1X:

```
DES-3028P:4#show 802.1x auth_state
Command: show 802.1x auth_state

Port    Auth PAE State  Backend State  Port Status
------  --------------  -------------  ------------
1       ForceAuth       Success        Authorized
2       ForceAuth       Success        Authorized
3       ForceAuth       Success        Authorized
4       ForceAuth       Success        Authorized
5       ForceAuth       Success        Authorized
6       ForceAuth       Success        Authorized
7       ForceAuth       Success        Authorized
8       ForceAuth       Success        Authorized
9       ForceAuth       Success        Authorized
10      ForceAuth       Success        Authorized
11      ForceAuth       Success        Authorized
12      ForceAuth       Success        Authorized
13      ForceAuth       Success        Authorized
14      ForceAuth       Success        Authorized
15      ForceAuth       Success        Authorized
16      ForceAuth       Success        Authorized
```

```
17      ForceAuth       Success        Authorized
18      ForceAuth       Success        Authorized
19      ForceAuth       Success        Authorized
20      ForceAuth       Success        Authorized

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

config 802.1x auth_mode

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

Example usage:

To configure 802.1X authentication by MAC address:

```
DES-3028P:4#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DES-3028P:4#
```

config 802.1x capability ports

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

Example usage:

To configure 802.1X capability on ports 1-10:

```
DES-3028P:4#config   802.1x   capability   ports   1–10
authenticator
Command:   config   802.1x   capability   ports   1–10
authenticator

Success.
```

```
DES-3028P:4#
```

config 802.1x auth_parameter

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

Example usage:

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

```
DES-3028P:4#config 802.1x auth_parameter ports 1–20 direction both
Command: config 802.1x auth_parameter ports 1–20 direction both

Success.

DES-3028P:4#
```

config 802.1x auth_protocol

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

Example usage:

To configure the authentication protocol on the Switch:

```
DES-3028P:4# config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DES-3028P:4#
```

config 802.1x init

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

Example usage:

To initialize the authentication state machine of all ports:

```
DES-3028P:4# config 802.1x init port_based
ports all
Command: config 802.1x init port_based ports
all

Success.

DES-3028P:4#
```

config 802.1x reauth

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

Example usage:

To configure 802.1X reauthentication for ports 1-18:

```
DES-3028P:4#config 802.1x reauth port_based ports 1-
18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-3028P:4#
```

config radius add

Purpose	Used to configure the settings the Switch will use to communicate with a RADIUS server.
Syntax	**config radius add <server_index 1-3> <server_ip> key <passwd 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}]**
Description	The **config radius add** command is used to configure the settings the Switch will use to communicate with a RADIUS server.
Parameters	*<server_index 1-3>* – 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.

config radius add

	<server_ip> – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key will be used between the Switch and the RADIUS server. *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. *default* – Uses the default UDP port number in both the “auth_port” and “acct_port” settings. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is *1812*. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is *1813*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DES-3028P:4#config radius add 1 10.48.74.121 key dlink
default
Command: config radius add 1 10.48.74.121 key dlink
default

Success.

DES-3028P:4#
```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.
Syntax	**config radius delete <server_index 1-3>**
Description	The **config radius delete** command is used to delete a previously entered RADIUS server configuration.
Parameters	*<server_index 1-3>* – Assigns a number to the current set of RADIUS server settings. Up to 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-3028P:4#config radius delete 1
Command: config radius delete 1

Success.

DES-3028P:4#
```

config radius

Purpose	Used to configure the Switch’s RADIUS settings.
Syntax	**config radius <server_index 1-3> {ipaddress <server_ip> | key <passwd 32> | auth_port <udp_port_number 1-65535> |**

config radius	
	acct_port <udp_port_number 1-65535>}
Description	The **config radius** command is used to configure the Switch's RADIUS settings.
Parameters	*<server_index 1-3>* – 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. *ipaddress <server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key will be used between the Switch and the RADIUS server. • *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is *1812*. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is *1813*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DES-3028P:4#config radius 1 10.48.74.121 key dlink
default
Command: config radius 1 10.48.74.121 key dlink
default

Success.

DES-3028P:4#
```

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

Example usage:

To configure the timeout option for radius servers.

```
DES-3028P:4# config radius parameter timeout 3
Command: config radius parameter timeout 3

Success.

DES-3028P:4#
```

show radius

Purpose	Used to display the current RADIUS configurations on the Switch.
Syntax	**show radius**
Description	The **show radius** 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-3028P:4#show radius
Command: show radius

Timeout      : 5 seconds
Retransmit   : 2

Index  IP Address          Auth-Port  Acct-Port  Status         Key
                           Number     Number
-----  -----------------   ---------  ---------  -------------  --------------
1       10.1.1.1             1812       1813       Active         switch
2       20.1.1.1             1800       1813       Active         des3226
3       30.1.1.1             1812       1813       Active         dlink

Total Entries : 3

DES-3028P:4#
```

create 802.1x guest_vlan

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

Example usage:

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

```
DES-3028P:4#create 802.1x guest_vlan Trinity
Command: create 802.1x guest_vlan Trinity

Success.

DES-3028P:4#
```

config 802.1x guest_vlan ports

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

Example usage:

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

```
DES-3028P:4#config 802.1x guest_vlan ports 1-5 state enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DES-3028P:4#
```

show 802.1x guest_vlan

Purpose	Used to view the configurations for a 802.1X Guest VLAN.
Syntax	**show 802.1x guest_vlan**
Description	The **show 802.1x guest_vlan** command is used to display the settings for the VLAN that has been enabled as an 802.1X Guest VLAN. Guest 802.1X VLAN clients are those who have not been authorized for 802.1X or they haven't yet installed the necessary 802.1X software, yet would still like to have limited access rights on the Switch.
Parameters	None.
Restrictions	None. This VLAN is only supported for port-based 802.1X and must have already been previously created using the **create vlan** command. Only one VLAN can be set as the 802.1X Guest VLAN.

Example usage:

To configure the configurations for a previously created 802.1X Guest VLAN.

```
DES-3028P:4#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-----------------------------------------------------------
Guest VLAN : Trinity
Enable guest VLAN ports: 1-5

DES-3028P:4#
```

delete 802.1x guest_vlan

Purpose	Used to delete a 802.1X Guest VLAN.
Syntax	**delete 802.1x guest_vlan {<vlan_name 32>}**
Description	The **delete 802.1x guest_vlan** command is used to delete an 802.1X Guest VLAN. Guest 802.1X VLAN clients are those who have not been authorized for 802.1X or they haven't yet installed the necessary 802.1X software, yet would still like to have limited access rights on the Switch.
Parameters	*<vlan_name 32>* – Enter the VLAN name of the Guest 802.1X VLAN to be deleted.
Restrictions	Only Administrator-level users can issue this command. Users must have already previously created a VLAN using the **create vlan** command. Only one VLAN can be set as the 802.1X Guest VLAN.

Example usage:

To delete a previously created 802.1X Guest VLAN.

```
DES-3028P:4#delete 802.1x guest_vlan Trinity
Command: delete 802.1x guest_vlan Trinity

Success.

DES-3028P:4#
```

show acct_client

Purpose	Used to display the current RADIUS accounting client.
Syntax	**show acct_client**
Description	The **show acct_client** command is used to display the current RADIUS accounting client currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS accounting client:

```
DES-3028P:4#show acct_client
Command: show acct_client

 radiusAcctClient
---------------------------------------------------------------------------------
 radiusAcctClientInvalidServerAddresses         0
 radiusAcctClientIdentifier                     D-Link

 radiusAuthServerEntry                          0
---------------------------------------------------------------------------------
 radiusAccServerIndex                           1
 radiusAccServerAddress                         10.53.13.199
 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 Enter Next Entry a All
```

show auth_client	
Purpose	Used to display the current RADIUS authentication client.
Syntax	**show auth_client**
Description	The **show auth_client** command is used to display the current RADIUS authentication client currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS authentication client:

```
DES-3028P:4#show auth_client
Command: show auth_client

radiusAuthClient
----------------------------------------------------------------------------------
radiusAuthClientInvalidServerAddresses       0
radiusAuthClientIdentifier                   D-Link

radiusAuthServerEntry                        0
----------------------------------------------------------------------------------
radiusAuthServerIndex                        : 1
radiusAuthServerAddress                      : 0.0.0.0
radiusAuthClientServerPortNumber               0
radiusAuthClientRoundTripTime                  0
radiusAuthClientAccessRequests                 0
radiusAuthClientAccessRetransmissions          0
radiusAuthClientAccessAccepts                  0
radiusAuthClientAccessRejects                  0
radiusAuthClientAccessChallenges               0
radiusAuthClientMalformedAccessResponses       0
radiusAuthClientBadAuthenticators              0
radiusAuthClientPendingRequests                0
radiusAuthClientTimeouts                       0
radiusAuthClientUnknownTypes                   0
radiusAuthClientPacketsDropped                 0
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

show auth_diagnostics

Purpose	Used to display the current authentication diagnostics.
Syntax	**show auth_diagnostics {ports [<auth_portlist>}**
Description	The **show auth_diagnostics** command is used to display the current authentication diagnostics of the Switch on a per port basis.
Parameters	*ports <auth_portlist>* – Specifies a range of ports.
Restrictions	None.

Example usage:

To display the current authentication diagnostics for port 1 of module 1:

```
DES-3028P:4#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

 Port number : 1

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

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

show auth_session_statistics

Purpose	Used to display the current authentication session statistics.
Syntax	**show auth_session_statistics {ports <auth_portlist | all>}**
Description	The **show auth_session** statistics command is used to display the current authentication session statistics of the Switch on a per port basis.
Parameters	*ports <auth_portlist>* – Specifies a range of ports. *all* – Specifies that all ports will be viewed.
Restrictions	None.

Example usage:

To display the current authentication session statistics for port 16 of module 1:

```
DES-3028P:4#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

 Port number : 1

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

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

show auth_statistics

Purpose	Used to display the current authentication statistics.
Syntax	**show auth_statistics {ports <auth_portlist>}**
Description	The **show auth_statistics** command is used to display the current authentication statistics of the Switch on a per port basis.
Parameters	*ports <auth_portlist>* – Specifies a range of ports.
Restrictions	None.

Example usage:

To display the current authentication statistics for port 1:16:

```
DES-3028P:4#show auth_statistics ports 1
Command: show auth_statistics ports 1

 Port number : 1

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

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

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

create 802.1x user

Purpose	Used to create a new 802.1X user.
Syntax	**create 802.1x user <username 15>**
Description	The **create 802.1x user** command is used to create new 802.1X users.
Parameters	*<username 15>* – A username of up to 15 alphanumeric characters in length.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an 802.1X user:

```
DES-3028P:4#create 802.1x user dtremblett
Command: create 802.1x user dtremblett

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

DES-3028P:4#
```

show 802.1x user

Purpose	Used to display the 802.1X user accounts on the Switch.
Syntax	**show 802.1x user**
Description	The **show 802.1x user** command is used to display the 802.1X Port-based or Host-based Network Access control local users currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view 802.1X users currently configured on the Switch:

```
DES-3028P:4#show 802.1x user
Command: show 802.1x user

Index                     UserName
--------------            --------------
Darren                    Trinity

Total Entries: 1

DES-3028P:4#
```

delete 802.1x user

Purpose	Used to delete an 802.1X user account on the Switch.
Syntax	**delete 802.1x user <username 15>**
Description	The **delete 802.1x user** command is used to delete the 802.1X Port-based or Host-based Network Access control local users currently

delete 802.1x user	
	configured on the Switch.
Parameters	*<username 15>* – A username can be as many as 15 alphanumeric characters.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete 802.1X users:

```
DES-3028P:4#delete 802.1x user dtremblett
Command: delete 802.1x user dtremblett

Are you sure to delete the user?(y/n)
Success.

DES-3028P:4#
```

22

ACCESS CONTROL LIST (ACL) COMMANDS

The DES-3028/28G/28P/52/52P implements Access Control Lists that enable the Switch to deny network access to specific devices or device groups based on IP settings and MAC address.

The access 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-ffffffffffff > | destination_mac <macmask 000000000000-ffffffffffff > | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp | igmp | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}] } | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff>} | 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> }] profile_id <value 1-256>
delete access_profile	[profile_id <value 1-256> | all]
config access_profile	<value 1-256> [add access_id [auto_assign | <value 1-65535>] [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp | igmp | 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>]} | packet_content offset <value 0-76> <hex0x0-0xffffffff> {offset <value 0-76> <hex 0x0-0xffffffff> {offset <value 0-76> <hex 0x0-0xffffffff> {offset <value 0-76> <hex 0x0-0xffffffff> {offset <value 0-76> <hex 0x0-0xffffffff>}}}}] port [<portlist> | all] [permit {priority <value 0-7> {replace_priority_with <value 0-7>} | rx_rate [no_limit |<value 64-1024000>]} | deny] {time_range <range_name 32>} | delete access_id <value 1-65535>]
show access_profile	profile_id <value 1-256>
enable cpu_interface_filtering	
disable cpu_interface_filtering	
create cpu access_profile profile_id	<value 1-3> [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp { type | code } | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}] } | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31<hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]
delete cpu access_profile	profile_id <value 1-3>
config cpu access_profile	<value 1-3> [add access_id <value 1-5> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> } | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> |code <value 0-255>} | igmp {type <value 0-255>}

Command	Parameters
	| tcp {src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define<hex 0x0-0xffffffff>}]} | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-5>]
show cpu access_profile	profile_id <value 1-3>

Access profiles allow users to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet’s header.

Creating an access profile is divided into two basic parts. First, an access profile must be created using the **create access_profile** command. For example, if users want to deny all traffic to the subnet 10.42.73.0 to 10.42.73.255, users must first **create** an access profile that instructs the Switch to examine all of the relevant fields of each frame.

First create an access profile that uses IP addresses as the criteria for examination:

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1 profile_name 1

Here we have created an access profile that will examine the IP field of each frame received by the Switch. Each source IP address the Switch finds will be combined with the **source_ip_mask** with a logical AND operation. The profile_id parameter is used to give the access profile an identifying number – in this case, 1 – and it is used to assign a priority in case a conflict occurs. The profile_id establishes a priority within the list of profiles. A lower profile_id gives the rule a higher priority. In case of a conflict in the rules entered for different profiles, the rule with the highest priority (lowest profile_id) will take precedence. *See below for information regarding limitations on access profiles and access rules.*

The **deny** parameter instructs the Switch to filter any frames that meet the criteria – in this case, when a logical AND operation between an IP address specified in the next step and the **ip_source_mask** match.

The default for an access profile on the Switch is to **permit** traffic flow. If users want to restrict traffic, users must use the **deny** parameter.

Now that an access profile has been created, users must add the criteria the Switch will use to decide if a given frame should be forwarded or filtered. We will use the **config access_profile** command to create a new rule that defines the criteria we want. Let’s further specify in the new rule to deny access to a range of IP addresses through an individual port: Here, we want to filter any packets that have an IP source address between 10.42.73.0 and 10.42.73.255, and specify the port that will not be allowed:

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny

We use the **profile_id 1** which was specified when the access profile was created. The **add** parameter instructs the Switch to add the criteria that follows to the list of rules that are associated with access profile 1. For each rule entered into the access profile, users can assign an access_id that identifies the rule within the list of rules. The access_id is an index number only and does not effect priority within the profile_id. This access_id may be used later if users want to remove the individual rule from the profile.

The **ip** parameter instructs the Switch that this new rule will be applied to the IP addresses contained within each frame’s header. **source_ip** tells the Switch that this rule will apply to the source IP addresses in each frame’s header. The IP address **10.42.73.1** will be combined with the **source_ip_mask 255.255.255.0** to give the IP address 10.42.73.0 for any source IP address between 10.42.73.0 to 10.42.73.255. Finally the restricted port - port number 7 - is specified.

create access_profile	
Purpose	Used to create an access profile on the Switch and to define which parts of each incoming frame’s header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create access_profile [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type}| ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp | igmp | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff>]} | 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**

create access_profile	
	<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>}] profile_id <value 1-256>
Description	The **create access_profile** 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	*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>* – Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format. *destination_mac <macmask>* – Specifies a MAC address mask for the destination MAC address. *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. *igmp* – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) 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 Universal Datagram Protocol (UDP) field. *src_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the source port. *dst_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the destination port.

create access_profile

	protocol_id_mask – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules. *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 the beginning of the packet to the 15th byte. *offset_16-31* – Enter a value in hex form to mask the packet from byte 16 to byte 31. *offset_32-*47 – Enter a value in hex form to mask the packet from byte 32 to byte 47. offset_48-63 – Enter a value in hex form to mask the packet from byte 48 to byte 63. offset_64-79 – Enter a value in hex form to mask the packet from byte 64 to byte 79. *profile_id <value 1-256>* – Sets the relative priority for the profile. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between *1* to *256*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an access list rules:

```
DES-3028P:4#create  access_profile  ip  vlan  source_ip_mask  20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp profile_id 101
Command:  create  access_profile  ip  vlan  source_ip_mask  20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp permit profile_id 101


Success.


DES-3028P:4#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile [profile_id <value 1-256> | all]**
Description	The **delete access_profile** command is used to delete a previously created access profile on the Switch.
Parameters	*profile_id <value 1-256>* – Enter an integer between *1* and *256* 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 *256*. *all* – Specifies all access list profiles will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3028P:4# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DES-3028P:4#
```

config access_profile

Purpose

Used to configure an access profile on the Switch and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the **create access_profile** command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.

Syntax

config access_profile profile_id <value 1-256> [add access_id [auto_assign | <value 1-65535>] [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> } | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp | igmp | 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>]} | packet_content offset <value 0-76> <hex0x0-0xffffffff> {offset <value 0-76> <hex 0x0-0xffffffff> {offset <value 0-76> <hex 0x0-0xffffffff> {offset <value 0-76> <hex 0x0-0xffffffff> {offset <value 0-76> <hex 0x0-0xffffffff>}}}}] port [<portlist> | all] [permit{ priority <value 0-7> replace_priority_with <value 0-7} | rx_rate [no_limit |<value 64-1024000>]} | deny] {time_range <range_name 32>} | delete access_id <value 1-65535>]

Description

The **config access_profile** command is used to configure an access profile on the Switch and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the **create access_profile** command, above.

Parameters

profile_id <value 1-256> – 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 *256*.

add access_id <value 1-65535> – Adds an additional rule to the above specified access profile. The value is used to index the rule created. For information on number of rules that can be created for a given port, please see the introduction to this chapter.

auto_assign – Choose this parameter to configure the Switch to automatically assign a numerical value (between *1* and *65535*) for the rule being configured.

ethernet – Specifies that the Switch will look only into the layer 2 part of each packet.

vlan <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN.

source_mac <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address.

destination_mac <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address.

802.1p <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.

ethernet_type <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

config access_profile	
Parameters	*ip* – Specifies that the Switch will look into the IP fields in each packet. *vlan <vlan_name 32>* – Specifies that the access profile will apply to only this VLAN. *source_ip <ipaddr>* – Specifies that the access profile will apply to only packets with this source IP address. *destination_id <value 0-255>* – 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. *igmp* – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet. *tcp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet. *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header. *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header. *flag_mask* – Enter the type of TCP flag to be masked. *all*: all flags are selected. *urg*: TCP control flag (urgent) *ack*: TCP control flag (acknowledgement) *psh*: TCP control flag (push) *rst*: TCP control flag (reset) *syn*: TCP control flag (synchronize) *fin*: TCP control flag (finish) *udp* – Specifies that the Switch will examine the Universal Datagram Protocol (UDP) field in each packet. src_port <value 0-65535> – *Specifies that the access profile will apply only to packets that have this UDP source port in their header.* dst_port <value 0-65535> – *Specifies that the access profile will apply only to packets that have this UDP destination port in their header.* *protocol_id <value 0-255>* – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules. *packet_content* – Specifies that the switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-76* – Enter a value in hex form to mask the packet from byte 0 to byte 76.
Parameters	*port <portlist>* – Specifies the port number on the Switch to permit or deny access for the rule. The user can also configure "all" to specify all ports. *permit* – Specifies that packets that match the access profile are permitted to be forwarded by the Switch. • *priority <value 0-7>* – This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. • *{replace_priority_with <value 0-7>}* – Enter this parameter if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. *rx_rate* – Use this to limit Rx bandwidth for the profile being configured. This rate is

config access_profile	
	implemented using the following equation – 64 value = 64kbit/sec. The user may select a value between 64- 1024000 or no limit. The default setting is no limit. *deny* – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered. *time_range <range_name 32>* – Choose this parameter and enter the name of the Time Range settings that has been previously configured using the **config time_range** command. This will set specific times when this access rule will be enabled or disabled on the Switch. *delete access_id <value 1-65535>* – Use this command to delete a specific ACL rule from the Ethernet profile, IP profile or packet_content profile. Up to 256 rules may be specified for all access profiles.
Restrictions	Only Administrator-level users can issue this command. Restriction: When the ACL rule is configured, the VLAN and DSCP cant be configured with source IP, destination IP or replace priority it can only be configured with DSCP.

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-3028P:4# config access_profile profile_id 1 add access_id 1 ip source_ip
10.42.73.1 port 7 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip
10.42.73.1 port 7 deny


Success.


DES-3028P:4#
```

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 explaination 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 1-256>**
Description	The **show access_profile** command is used to display the currently configured access profiles.
Parameters	*profile_id <value 1-256>* – 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 *256.*
Restrictions	None.

Example usage:

To display all of the currently configured access profiles on the Switch:

```
DES-3028P:4#show access_profile
Command: show access_profile

Access Profile Table

================================================================================
Profile ID: 101                        Type: IPv4 Frame Filter - ICMP
================================================================================
Masks  Option
VLAN             Source IP       Dest. IP        DSCP Prot
---------------- --------------- --------------- ---- ----
                 20.0.0.0        10.0.0.0             ICMP

================================================================================
Total Profile Entries: 1

Total Used Rule Entries: 0

Total Unused Rule Entries: 256

DES-3028P:4#
```

create cpu access_profile	
Purpose	Used to create an access profile specifically for **CPU Interface Filtering** on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.
Syntax	**create cpu access_profile <value 1-3> [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp { type } | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}] } | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define <hex 0x0-0xffffffff>}]}| packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31<hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff><hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]**
Description	The **create cpu access_profile** command is used to create an access profile used only for CPU Interface Filtering. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.
Parameters	*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>* – Specifies to examine the source MAC address mask. • *destination_mac <macmask>* – 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

create cpu access_profile

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 frames Transport Control Protocol (TCP) field.

  src_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.

  dst_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.

  flag_mask [all | {urg | ack | psh | rst | syn | fin}] – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between **all**, **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize) and **fin** (finish).
- *udp* – Specifies that the switch will examine each frame’s Universal Datagram Protocol (UDP) field.

  src_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.

  dst_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.
- *protocol_id_mask <hex 0x0-0xff>* – Specifies that the Switch will examine each frame’s Protocol ID field using the hex form entered here.
- *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.
- *packet_content_mask* – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows:
  - *offset_0-15* – Enter a value in hex form to mask the packet from byte 0 to byte 15.
  - *offset_16-31* – Enter a value in hex form to mask the packet from byte 16 to byte 31.
  - *offset_32-47* – Enter a value in hex form to mask the packet from byte 32 to byte 47.
  - *offset_48-63* – Enter a value in hex form to mask the packet from byte 48 to byte 63.
  - *offset_64-79* – Enter a value in hex form to mask the packet from byte 64 to byte 79.

profile_id <value 1-3> – Enter an integer between *1* and *3* that is used to identify the CPU access profile to be created with this command.

Restrictions — Only Administrator-level users can issue this command.

Example usage:

To create a CPU access profile:

```
DES-3028P:4# create cpu access_profile profile_id 1 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type
code
Command: create cpu access_profile profile_id 1 ip vlan source_ip_mask
20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DES-3028P:4#
```

delete cpu access_profile	
Purpose	Used to delete a previously created CPU access profile.
Syntax	**delete cpu access_profile profile_id <value 1-3>**
Description	The **delete cpu access_profile** command is used to delete a previously created CPU access profile.
Parameters	*profile_id* <*value 1-3*> – Enter an integer between *1* and *3* that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DES-3028P:4#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3028P:4#
```

config cpu access_profile	
Purpose	Used to configure a CPU access profile used for CPU Interface Filtering and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the **create cpu access_profile** command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.
Syntax	**config cpu access_profile profile_id <value 1-3> [add access_id <value 1-5> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> } | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin } | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define<hex 0x0-0xffffffff>}]} | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> }] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-5>]**
Description	The **config cpu access_profile** command is used to configure a CPU access profile for CPU Interface Filtering and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the **create cpu access_profile** command, above.
Parameters	*profile_id* <*value 1-3*> – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority. *add access_id* <*value 1-5*> – Adds an additional rule to the above specified access profile.

config cpu access_profile	
	The value is used to index the rule created. *ethernet* – Specifies that the Switch will look only into the layer 2 part of each packet. *vlan <vlan_name 32>* – Specifies that the access profile will apply to only to this VLAN. *source_mac <macaddr>* – Specifies that the access profile will apply to this source MAC address. *destination_mac <macaddr>* – Specifies that the access profile will apply to this destination MAC address. *ethernet_type <hex 0x0-0xffff>* – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header. *ip* – Specifies that the Switch will look into the IP fields in each packet. *vlan <vlan_name 32>* – Specifies that the access profile will apply to only this VLAN. *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. *igmp* – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet. *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. *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 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 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_0-76* - Enter a value in hex form to mask the packet from byte 0 to byte 76.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *permit* | *deny* – Specify that the packet matching the criteria configured with command will either be permitted entry to the cpu or denied entry to the CPU. *time_range <range_name 32>* – Choose this parameter and enter the name of the Time Range settings that has been previously configured using the **config time_range** command. This will set specific times when this access rule will be enabled or disabled on the Switch. *delete access_id <value 1-5>* – Use this to remove a previously created access rule in a

config cpu access_profile	
	profile ID.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure CPU access list entry:

```
DES-3028P:4#config cpu access_profile profile_id 3 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port all
deny
Command: config cpu access_profile profile_id 3 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port all
deny

Success.

DES-3028P:4#
```

delete cpu access_profile	
Purpose	Used to delete a previously created CPU access profile.
Syntax	**delete cpu access_profile profile_id <value 1-3>**
Description	The **delete cpu access_profile** command is used to delete a previously created CPU access profile.
Parameters	*profile_id <value 1-3>* – Enter an integer between 1 and 3 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DES-3028P:4#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3028P:4#
```

show cpu access_profile	
Purpose	Used to view the CPU access profile entry currently set in the Switch.
Syntax	**show cpu access_profile profile_id <value 1-3>**
Description	The **show cpu access_profile** command is used view the current CPU interface filtering entries set on the Switch.
Parameters	*profile_id <value 1-3>* – Enter an integer between *1* and *3* that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command.
Restrictions	None.

Example usage:

To show the CPU filtering state on the Switch:

```
DES-3028P:4#show cpu access_profile profile_id 2
Command: show cpu access_profile profile_id 2

CPU Interface Filtering state: Disabled

Access Profile Table
=============================================
Total Profile Entries: 0
Total Rule Entries:  0

DES-3028P:4#
```

enable cpu_interface_filtering

Purpose	Used to enable CPU interface filtering on the Switch.
Syntax	**enable cpu_interface_filtering**
Description	This command is used, in conjunction with the **disable cpu_interface_filtering** command below, to enable and disable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To enable CPU interface filtering:

```
DES-3028P:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3028P:4#
```

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-level users can issue this command.

Example Usage:

To disable CPU filtering:

```
DES-3028P:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-3028P:4#
```

23

TIME RANGE COMMANDS

The Time Range commands are used in conjunction with the Access Profile commands listed in the previous chapter to determine a starting point and an ending point, based on days of the week, when an Access Profile configuration will be enabled on the Switch. Once configured here, the time ranges will to be applied to an access profile rule using the **config access_profile profile_id** command.

NOTE: The Time Range commands are based on the time settings of the Switch. Make sure to configure the time for the Switch appropriately for these commands using commands listed in the following chapter, **Time and SNTP Commands**.

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

Command	Parameters
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	

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

config time_range	
Purpose	Used to configure a time range in which an access profile rule is to be enabled.
Syntax	**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 is to be used in conjunction with an access profile rule to determine a period of time when an access profile and an associated rule are to be enabled on the Switch. Remember, this time range can only be applied to one period of time and also, it is based on the time set on the Switch.
Parameters	*<range_name 32>* – Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the **config access_profile profile_id** command to identify the access profile and associated rule to be enabled for this time range. *hours* – This parameter is used to set the time in the day that this time range is to be set using the following parameters: *start time <time hh:mm:ss>* – Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. *end time <time hh:mm:ss>* – Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system. *weekdays* – Use this parameter to determine the days of the week to set this time range. *<daylist>* – The user may set the days of the week here to set this time range in the three letter format (mon, tue, wed…). To specify a day range, separate the daylist using a dash (mon-fri would mean Monday through Friday). To specify a list of days in a week, separate the daylist using a comma, with no spaces (mon,tue,fri would mean Monday, Tuesday and Friday). *delete* – Use this parameter to delete a previously configured time range from the system.

config time_range

Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the time range time1 to be between 6:30 a.m. and 9:40 p.m., Monday to Friday:

```
DES-3028P:4#config time_range time1 hours start_time 6:30:00
end_time 21:40:00 weekdays mon-fri
Command: config time_range time1 hours start_time 6:30:00
end_time 21:40:00 weekdays mon-fri

Success.

DES-3028P:4#
```

show time_range

Purpose	To view the current configurations of the time range set on the Switch.
Syntax	**show time_range**
Description	This command is used to display the currently configured time range(s) set on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the current time range settings.

```
DES-3028P:4#show time_range
Command: show time_range

Time Range information
--------------------------------------------
Range name   : time1
Weekdays     : Mon,Tue,Wed,Thu,Fri
Start time   : 06:30:00
End time     : 21:40:00

Total entries: 1

DES-3028P:4#
```

24

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 create trusted_host explained in the previous section. Once the user configures these acceptable IP addresses, other packets containing different IP addresses will be dropped by the Switch, thus limiting the bandwidth of IP packets

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

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

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

config safeguard_engine	
Purpose	To configure ARP storm control for system.
Syntax	**{state [enable | disable] | utilization {rising <value 20-100> | falling <value 20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}**
Description	Use this command to configure Safeguard Engine to minimize the effects of an ARP storm.
Parameters	*state [enable | disable]* – Select the running state of the Safeguard Engine function as enable or disable. *cpu_utilization* – Select this option to trigger the Safeguard Engine function to enable based on the following determinates: *rising <value 20-100>* – The user can set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises to this percentage, the Safeguard Engine mechanism will initiate. *falling <value 20-100>* – The user can set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to this percentage, the Safeguard Engine mechanism will shut down. *trap_log [enable | disable]* – Choose whether to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate. *mode [strict | fuzzy]* – Toggle between *strict* and *fuzzy* mode. *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.

config safeguard_engine

Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the safeguard engine for the Switch:

```
DES-3028P:4#config safeguard_engine state enable utilization rising
45
Command: config safeguard_engine state enable utilization rising 45

Success.

DES-3028P:4#
```

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-3028P:4#show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State           :  Disabled
Safeguard Engine Current Status  :  Normal mode
=======================================================
CPU utilization information:
Rising Threshold (20-100)                 : 30%
Falling Threshold (20-100)                : 20%
Trap/Log State                            : Disabled
Mode
: Fuzzy

DES-3028P:4#
```

25

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>] forward_list [null | <portlist>]
show traffic_segmentation	<portlist>

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

config traffic_segmentation	
Purpose	Used to configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation [<portlist>] forward_list [null | <portlist>]**
Description	The **config traffic_segmentation** command is used to configure traffic segmentation on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports that will be configured for traffic segmentation. *forward_list* – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above. • *null* – No 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-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-3028P:4#config traffic_segmentation 1-10 forward_list
11-15
Command:  config  traffic_segmentation  1-10  forward_list
11-15

Success.

DES-3028P:4#
```

show traffic_segmentation	
Purpose	Used to display the current traffic segmentation configuration on the Switch.
Syntax	**show traffic_segmentation <portlist>**
Description	The **show traffic_segmentation** 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.

show traffic_segmentation	
Restrictions	The port lists for segmentation and the forward list must be on the same Switch.

Example usage:

To display the current traffic segmentation configuration on the Switch.

```
DES-3028P:4#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port    Forward Portlist
----    ----------------------------
1         1-28
2         1-28
3         1-28
4         1-28
5         1-28
6         1-28
7         1-28
8         1-28
9         1-28
10        1-28
11        1-28
12        1-28
13        1-28
14        1-28
15        1-28
16        1-28
17        1-28
18        1-28
CTRL+C  ESC  q  Quit  SPACE  n  Next  Page  ENTER  Next
Entry a All
```

26

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>}
show sntp	
enable sntp	
disable sntp	
config time	<date ddmmmyyyy > <time hh:mm:ss >
config time_zone	{operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst	[disable | repeating {s_week <start_week 1-4,last> | s_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>}**
Description	Use this command to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable sntp).
Parameters	*primary* – This is the primary server from which the SNTP information will be taken. *<ipaddr>* – The IP address of the primary server. *secondary* – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable. *<ipaddr>* – The IP address for the secondary server. *poll-interval <int 30-99999>* – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.
Restrictions	Only Administrator-level users can issue this command. SNTP service must be enabled for this command to function (*enable sntp*).

Example usage:

To configure SNTP settings:

```
DES-3028P:4#config  sntp  primary  10.1.1.1  secondary  10.1.1.2
poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-
interval 30

Success.

DES-3028P:4#
```

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-3028P:4#show sntp
Command: show sntp

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

DES-3028P:4#
```

enable sntp

Purpose	To enable SNTP server support.
Syntax	**enable sntp**
Description	This will enable SNTP support. SNTP service must be separately configured (see **config sntp**). Enabling and configuring SNTP support will override any manually configured system time settings.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command. SNTP settings must be configured for SNTP to function (**config sntp**).

Example usage:

To enable the SNTP function:

```
DES-3028P:4#enable sntp
Command: enable sntp

Success.

DES-3028P:4#
```

disable sntp

Purpose	To disable SNTP server support.
Syntax	**disable sntp**
Description	This will disable SNTP support. SNTP service must be separately configured (see **config sntp**).
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SNTP support:

```
DES-3028P:4#disable sntp
Command: disable sntp

Success.

DES-3028P:4#
```

config time

Purpose	Used to manually configure system time and date settings.
Syntax	**config time <date ddmmmyyyy> <time hh:mm:ss>**
Description	This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	*date* – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003. *time* – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.
Restrictions	Only Administrator-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
DES-3028P:4#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3028P:4#
```

config time_zone

Purpose	Used to determine the time zone used in order to adjust the system clock.
Syntax	**config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}**
Description	This will adjust system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	*operator* – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT. *hour* – Select the number of hours different from GMT. *min* – Select the number of minutes difference added or subtracted to adjust the time zone.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DES-3028P:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3028P:4#
```

config dst	
Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	**config dst [disable | repeating {s_week <start_week 1-4,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.
Parameters	*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. • *<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-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
 DES-3028P:4#config dst repeating s_week 2 s_day tue
s_mth 4 s_time 15:00 e_week 2 e_day wed e_mth 10 e_time
15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth
4 s_time 15:00 e_week 2 e_day wed e_mth 10 e_time 15:30
offset 30


Success.


DES-3028P:4#
```

show time

Purpose	Used to display the current time settings and status.
Syntax	**show time**
Description	This will display 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-3028P:4#show time
Command: show time

Current Time Source : System Clock
Current Time        : 1 Days 01:39:17
Time Zone           : GMT +02:30
Daylight Saving Time: Repeating
Offset in minutes   : 30
    Repeating From  : Apr 2nd Tue 15:00
    To              : Oct 2nd Wed 15:30
    Annual    From  : 29 Apr 00:00
    To              : 12 Oct 00:00

DES-3028P:4#
```

27

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 [System] | ipaddress <ipaddr> | static}
config arp_aging time	<value 0-65535>
clear arptable	

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-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-3028P:4#create  arpentry  10.48.74.121  00-50-BA-00-
07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DES-3028P:4#
```

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 above.

config arpentry

Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To configure a static ARP entry for the IP address 10.48.74.12 and MAC address 00:50:BA:00:07:36:

```
DES-3028P:4#config arpentry 10.48.74.12 00-50-BA-
00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-
07-36

Success.

DES-3028P:4#
```

delete arpentry

Purpose	Used to delete a static entry into the ARP table.
Syntax	**delete arpentry {[<ipaddr> | all]}**
Description	This command is used to delete a static ARP entry, made using the **create arpentry** command above, by specifying either the IP address of the entry or all. Specifying *all* clears the Switch’s ARP table.
Parameters	*<ipaddr>* – The IP address of the end node or station. *all* – Deletes all ARP entries.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

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

```
DES-3028P:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-3028P:4#
```

config arp_aging time

Purpose	Used to configure the age-out timer for ARP table entries on the Switch.
Syntax	**config arp_aging time <value 0-65535>**
Description	This command sets the maximum amount of time, in minutes, that an ARP entry can remain in the Switch’s ARP table, without being accessed, before it is dropped from the table.
Parameters	*time <value 0-65535>* – The ARP age-out time, in minutes. The value may be set in the range of 0-65535 minutes with a default setting of 20 minutes.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```
DES-3028P:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3028P:4#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	**show arpentry {ipif [System] | ipaddress <ipaddr> | static}**
Description	This command is used to display the current contents of the Switch's ARP table.
Parameters	*ipif [System]* – The name of the IP interface, the end node or station for which the ARP table entry was made, resides on. *ipaddress <ipaddr>* – The network address corresponding to the IP interface name above. *static* – Displays the static entries to the ARP table.
Restrictions	None.

Example Usage:

To display the ARP table**:**

```
DES-3028P:4#show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface      IP Address       MAC Address        Type
-------------  ---------------  -----------------  ---------------
System         10.0.0.0         FF-FF-FF-FF-FF-FF  Local/Broadcast
System         10.6.51.15       00-1D-60-E7-B5-CD  Dynamic
System         10.22.8.50       00-80-C8-DF-E8-EE  Dynamic
System         10.30.28.112     00-30-28-01-12-02  Dynamic
System         10.39.77.24      08-00-01-43-00-00  Dynamic
System         10.44.8.253      00-44-08-FD-09-09  Dynamic
System         10.53.7.12       00-50-BA-11-11-04  Dynamic
System         10.56.85.10      00-0E-A6-8F-72-EA  Dynamic
System         10.67.33.67      00-00-E2-58-DB-CF  Dynamic
System         10.71.77.126     00-04-96-20-D5-25  Dynamic
System         10.73.21.11      00-19-5B-EF-78-B5  Local
System         10.73.60.106     00-00-00-11-12-13  Dynamic
System         10.90.90.90      00-21-91-21-34-03  Dynamic
System         10.255.255.255   FF-FF-FF-FF-FF-FF  Local/Broadcast

Total Entries  : 14

DES-3028P:4#
```

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-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
DES-3028P:4#clear arptable
Command: clear arptable

Success.

DES-3028P:4#
```

28

ROUTING TABLE COMMANDS

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

Command	Parameters
create iproute	[default] <ipaddr> {<metric 1-65535>}
delete iproute	[default]
show iproute	{<network_address> | static}

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

create iproute default	
Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	**create iproute [default] <ipaddr> {<metric 1-65535>}**
Description	This command is used to create a default static IP route entry to the Switch's IP routing table.
Parameters	*<ipaddr>* – The gateway IP address for the next hop router. *<metric 1-65535>* – Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add the default static address 10.48.74.121, with a metric setting of 1, to the routing table:

```
DES-3028P:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DES-3028P:4#
```

delete iproute default	
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	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the default IP route 10.53.13.254:

```
DES-3028P:4#delete iproute default 10.53.13.254
Command: delete iproute default 10.53.13.254

Success.

DES-3028P:4#
```

show iproute	
Purpose	Used to display the Switch’s current IP routing table.
Syntax	**show iproute {<network_address> | static}**
Description	This command will display the Switch’s current IP routing table.
Parameters	*<network_address>* – The network IP address. *static* – Select a static IP route.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DES-3028P:4#show iproute
Command: show iproute

Routing Table

IP Address/Netmask     Gateway      Interface    Hops    Protocol
---------------        ----------   -----------  ----    -----------
0.0.0.0                10.1.1.254    System       1       Default
10.0.0.0/8             10.48.74.122  System       1       Local

Total Entries: 2

DES-3028P:4#
```

29

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

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

enable mac_notification

Purpose	Used to enable global MAC address table notification on the Switch.
Syntax	**enable mac_notification**
Description	This command is used to enable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable MAC notification without changing basic configuration:

```
DES-3028P:4#enable mac_notification
Command: enable mac_notification

Success.

DES-3028P:4#
```

disable mac_notification

Purpose	Used to disable global MAC address table notification on the Switch.
Syntax	**disable mac_notification**
Description	This command is used to disable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable MAC notification without changing basic configuration:

```
DES-3028P:4#disable mac_notification
Command: disable mac_notification

Success.
```

```
DES-3028P:4#
```

config mac_notification

Purpose	Used to configure MAC address notification.
Syntax	**config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}**
Description	MAC address notification is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*interval <sec 1-2147483647>* – The time in seconds between notifications. The user may choose an interval between 1 and 2,147,483,647 seconds. *historysize <1-500>* – The maximum number of entries listed in the history log used for notification.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the Switch’s MAC address table notification global settings:

```
DES-3028P:4#config   mac_notification   interval   1
historysize 500
Command:   config   mac_notification   interval   1
historysize 500

Success.

DES-3028P:4#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist> | all] [enable | disable]**
Description	MAC address notification is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *all* – Entering this command will set all ports on the system. *[enable | disable]* – These commands will enable or disable MAC address table notification on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DES-3028P:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-3028P:4#
```

show mac_notification

Purpose	Used to display the Switch’s MAC address table notification global settings.
Syntax	**show mac_notification**
Description	This command is used to display the Switch’s MAC address table notification global settings.
Parameters	None.
Restrictions	None.

Example usage:

To view the Switch’s MAC address table notification global settings:

```
DES-3028P:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State          : Enabled
Interval       : 1
History Size   : 1

DES-3028P:4#
```

show mac_notification ports

Purpose	Used to display the Switch’s MAC address table notification status settings.
Syntax	**show mac_notification ports <portlist>**
Description	This command is used to display the Switch’s MAC address table notification status settings.
Parameters	*<portlist>* – Specify a port or group of ports to be viewed. Entering this command without the parameter will display the MAC notification table for all ports.
Restrictions	None.

Example usage:

To display all port’s MAC address table notification status settings:

```
DES-3028P:4#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------  -------------------------------------------
1                                 Disabled
2                                 Disabled
3                                 Disabled
4                                 Disabled
5                                 Disabled
6                                 Disabled
7                                 Disabled
8                                 Disabled
9                                 Disabled
```

```
10                             Disabled
11                             Disabled
12                             Disabled
13                             Disabled
14                             Disabled
15                             Disabled
16                             Disabled
17                             Disabled
18                             Disabled
19                             Disabled
20                             Disabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r
Refresh
```

30

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

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-3028P:4#enable authen_policy
Command: enable authen_policy

Success.

DES-3028P:4#
```

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-3028P:4#disable authen_policy
Command: disable authen_policy

Success.

DES-3028P:4#
```

show authen_policy

Purpose	Used to display the system access authentication policy status on the Switch.
Syntax	**show authen_policy**
Description	This command will show the current status of the access authentication policy on the Switch.
Parameters	None.

show authen_policy

Restrictions	None.

Example usage:

To display the system access authentication policy:

```
DES-3028P:4#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DES-3028P:4#
```

create authen_login method_list_name

Purpose	Used to create a user defined method list of authentication methods for users logging on to the Switch.
Syntax	**create authen_login method_list_name <string 15>**
Description	This command is used to create a list for authentication techniques for user login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the method list “Trinity.”:

```
DES-3028P:4#create     authen_login     method_list_name
Trinity
Command: create authen_login method_list_name Trinity

Success.

DES-3028P:4#
```

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}**
Description	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 *tacacs – xtacacs – local,* the Switch will send an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the

config authen_login	
	same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local* account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch. Successful login using any of these methods will give the user a “user” privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the *enable admin* command, followed by a previously configured password. (*See the **enable admin** part of this section for more detailed information, concerning the **enable admin** command.)*
Parameters	*default* – The default method list for access authentication, as defined by the user. The user may choose one or a combination of up to four(4) of the following authentication methods: ▪ *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from the remote TACACS *server hosts* of the TACACS *server group* list. ▪ *xtacacs* – Adding this parameter will require the user to be authenticated using the *XTACACS* protocol from the remote XTACACS *server hosts* of the XTACACS *server group* list. ▪ *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. ▪ *radius* – Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. ▪ *server_group <string 15>* – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. ▪ *local* – Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch. ▪ *none* – Adding this parameter will require no authentication to access the Switch. *method_list_name* – Enter a previously implemented method list name defined by the user. The user may add one, or a combination of up to four (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* – 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.

config authen_login

	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, in that order.

```
DES-3028P:4#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-3028P:4#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DES-3028P:4#config  authen_login  default  method  xtacacs
tacacs+ local
Command:  config  authen_login  default  method  xtacacs
tacacs+ local

Success.

DES-3028P:4#
```

delete authen_login method_list_name

Purpose	Used to delete a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**delete authen_login method_list_name <string 15>**
Description	This command is used to delete a list for authentication methods for user login.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list* to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the method list name “Trinity”:

```
DES-3028P:4#delete     authen_login     method_list_name
Trinity
Command: delete authen_login method_list_name Trinity

Success.

DES-3028P:4#
```

show authen_login

Purpose	Used to display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**show authen_login [default | method_list_name <string 15> | all]**
Description	This command is used to show a list of authentication methods for user login.
Parameters	*default* – Entering this parameter will display the default method list for users logging on to the Switch. *method_list_name <string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list* to view. *all* – Entering this parameter will display all the authentication login methods currently configured on the Switch. The window will display the following parameters: ▪ Method List Name – The name of a previously configured method list name. ▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest). ▪ Method Name – Defines which security protocols are implemented, per method list name. ▪ Comment – Defines the type of Method. *User-defined Group* refers to server group defined by the user. *Built-in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS / XTACACS / TACACS+ / RADIUS which are local (authentication through the user account on the Switch) and none (no authentication necessary to access any function on the Switch).
Restrictions	None.

Example usage:

To view the authentication login method list named Trinity:

```
DES-3028P:4#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-3028P:4#
```

create authen_enable method_list_name

Purpose	Used to create a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**create authen_enable method_list_name <string 15>**
Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the

create authen_enable method_list_name

	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 (8) enable method lists can be implemented on the Switch.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *enable method list* to create.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a user-defined method list, named “Permit” for promoting user privileges to Administrator privileges:

```
DES-3028P:4#create    authen_enable    method_list_name
Permit
Command: create authen_enable method_list_name Permit

Success.

DES-3028P:4#
```

config authen_enable

Purpose	Used to configure a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}**
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 (8) enable method lists can be implemented simultaneously on the Switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local_enable,* the Switch will send an authentication request to the first *TACACS* host in the server group. If no verification is found, the Switch will send an authentication request to the second *TACACS* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local_enable* password set in the Switch is used to authenticate the user. Successful authentication using any of these methods will give the user an “Admin” level privilege.
Parameters	*default* – The default method list for administration rights authentication, as defined by the user. The user may choose one or a combination of up to four (4) of the following authentication methods: ▪ *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from the remote TACACS *server hosts* of the TACACS *server group* list.

config authen_enable	
	▪ *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_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, in that order.

```
DES-3028P:4#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-3028P:4#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DES-3028P:4#config  authen_enable  default  method  xtacacs  tacacs+
local
Command: config authen_enable default method xtacacs tacacs+ local

Success.

DES-3028P:4#
```

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	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *enable method list* to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user-defined method list "Permit"

```
DES-3028P:4#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DES-3028P:4#
```

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 delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	*default* – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the Switch. *method_list_name <string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to view. all – Entering this parameter will display all the authentication login methods currently configured on the Switch. The window will display the following parameters: ▪ Method List Name – The name of a previously configured method list name.

show authen_enable

	▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest). ▪ Method Name – Defines which security protocols are implemented, per method list name. ▪ Comment – Defines the type of Method. *User-defined Group* refers to *server groups* defined by the user. *Built-in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the *local_enable* password on the Switch) and none (no authentication necessary to access any function on the Switch).
Restrictions	None.

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DES-3028P:4#show authen_enable all
Command: show authen_enable all

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

default              1        tacacs+         Built-in Group
                     2        local           Keyword

Total Entries : 2

DES-3028P:4#
```

config authen application

Purpose	Used to configure various applications on the Switch for authentication using a previously configured method list.
Syntax	**config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]**
Description	This command is used to configure Switch configuration applications (console, telnet, ssh, web) for login at the user level and at the administration level (*authen_enable*) utilizing a previously configured method list.
Parameters	*application* – Choose the application to configure. The user may choose one of the following five options to configure. ▪ *console* – Choose this parameter to configure the command line interface login method. ▪ *telnet* – Choose this parameter to configure the telnet login method. ▪ *ssh* – Choose this parameter to configure the Secure

config authen application	
	Shell login method. ▪ *http* – Choose this parameter to configure the web interface login method. ▪ *all* – Choose this parameter to configure all applications (console, telnet, ssh, web) login method. *login* – Use this parameter to configure an application for normal login on the user level, using a previously configured method list. *enable* – Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Use this parameter to configure an application for user authentication using the default method list. *method_list_name <string 15>* – Use this parameter to configure an application for user authentication using a previously configured method list. Enter an alphanumeric string of up to 15 characters to define a previously configured method list.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the web interface:

```
DES-3028P:4#config  authen  application  http  login
default
Command:  config  authen  application  http  login
default


Success.


DES-3028P:4#
```

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-3028P:4#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-3028P:4#
```

create authen server_host

Purpose	Used to create an authentication server host.
Syntax	**create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 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	*server_host <ipaddr>* – The IP address of the remote server host to add. *protocol* – The protocol used by the server host. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* – Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1-65535>* – Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *key <key_string 254>* – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters. *timeout <int 1-255>* – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond.
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-3028P:4#create authen server_host 10.1.1.121 protocol
tacacs+ port 1234 timeout 10 retransmit 5
Command:  create  authen  server_host  10.1.1.121  protocol
tacacs+ port 1234 timeout 10 retransmit 5
```

```
Success.

DES-3028P:4#
```

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>}**
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	*server_host <ipaddr>* – The IP address of the remote server host the user wishes to alter. *protocol* – The protocol used by the server host. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ radius – Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1-65535>* – Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *key <key_string 254>* – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters or choose none. *timeout <int 1-255>* – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond. This field is inoperable for the TACACS+ protocol.
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-3028P:4#config    authen    server_host    10.1.1.121
protocol tacacs+ port 4321 timeout 12 retransmit 4
Command:  config  authen  server_host  10.1.1.121  protocol
tacacs+ port 4321 timeout 12 retransmit 4

Success.

DES-3028P:4#
```

delete authen server_host

Purpose	Used to delete a user-defined authentication server host.
Syntax	**delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command is used to delete a user-defined authentication server host previously created on the Switch.
Parameters	*server_host <ipaddr>* – The IP address of the remote server host to be deleted. *protocol* – The protocol used by the server host the user wishes to delete. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol*.* ▪ *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* – 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-3028P:4#delete authen server_host 10.1.1.121 protocol
tacacs+
Command:  delete  authen  server_host  10.1.1.121  protocol
tacacs+

Success.

DES-3028P:4#
```

show authen server_host

Purpose	Used to view a user-defined authentication server host.
Syntax	**show authen server_host**
Description	This command is used to view user-defined authentication server hosts previously created on the Switch. The following parameters are displayed: *IP Address* – The IP address of the authentication server host. *Protocol* – The protocol used by the server host. Possible results will include TACACS, XTACACS, TACACS+ or RADIUS. *Port* – The virtual port number on the server host. The default value is

show authen server_host

	49. *Timeout* – The time in seconds the Switch will wait for the server host to reply to an authentication request. *Retransmit* – The value in the retransmit field denotes how many times the device will resend an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol. *Key* – Authentication key to be shared with a configured TACACS+ server only.
Parameters	None.
Restrictions	None.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DES-3028P:4#show authen server_host
Command: show authen server_host

IP Address    Protocol    Port  Timeout  Retransmit  Key
------------ --------     ----- -------  ----------  -------------
10.53.13.94    TACACS       49     5         2       No Use

Total Entries : 1

DES-3028P:4#
```

create authen server_group

Purpose	Used to create a user-defined authentication server group.
Syntax	**create authen server_group <string 15>**
Description	This command 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 (8) authentication server hosts to this group using the **config authen server_group** command.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the newly created server group.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the server group “group_1”:

```
DES-3028P:4#create authen server_group group_1
Command: create authen server_group group_1

Success.

DES-3028P:4#
```

config authen server_group

Purpose	Used to configure a user-defined authentication server group.
Syntax	**config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command 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	*server_group* – The user may define the group by protocol groups built into the Switch (TACACS/XTACACS/TACACS+/RADIUS), or by a user-defined group previously created using the *create authen server_group* command. ▪ *tacacs* – Use this parameter to utilize the built-in TACACS server protocol on the Switch. Only server hosts utilizing the TACACS protocol may be added to this group. ▪ *xtacacs* – Use this parameter to utilize the built-in XTACACS server protocol on the Switch. Only server hosts utilizing the XTACACS protocol may be added to this group. ▪ *tacacs+* – Use this parameter to utilize the built-in TACACS+ server protocol on the Switch. Only server hosts utilizing the TACACS+ protocol may be added to this group. ▪ *radius* – Use this parameter to utilize the built-in RADIUS server protocol on the Switch. Only server hosts utilizing the RADIUS protocol may be added to this group. ▪ *<string 15>* – Enter an alphanumeric string of up to 15 characters to define the previously created server group. This group may add any combination of server hosts to it, regardless of protocol. *add/delete* – Enter the correct parameter to add or delete a server host from a server group. *server_host <ipaddr>* – Enter the IP address of the previously configured server host to add or delete. *protocol* – Enter the protocol utilized by the server host. There are three options: ▪ *tacacs* – Use this parameter to define the protocol if the server host is using the TACACS authentication protocol. ▪ *xtacacs* – Use this parameter to define the protocol if the server host is using the XTACACS authentication protocol. ▪ *tacacs+* – Use this parameter to define the protocol if the server host is using the TACACS+ authentication protocol. ▪ *radius* – 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-3028P:4#  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-3028P:4#
```

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-3028P:4#delete server_group group_1
Command: delete server_group group_1

Success.

DES-3028P:4#
```

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	None.

Example usage:

To view authentication server groups currently set on the Switch.

```
DES-3028P:4#show authen server_group
Command: show authen server_group

Group Name    IP Address                        Protocol
-----------  -----------------------------    ------------
radius       ---------------------------------------------------------
tacacs       ---------------------------------------------------------
tacacs+      ---------------------------------------------------------
xtacacs      ---------------------------------------------------------

Total Entries : 4

DES-3028P:4#
```

config authen parameter response_timeout

Purpose	Used to configure the amount of time the Switch will wait for a user to enter authentication before timing out.
Syntax	**config authen parameter response_timeout <int 0-255>**
Description	This command will set the time the Switch will wait for a response of authentication from the user.
Parameters	*response_timeout <int 0-255>* – Set the time, in seconds, the Switch will wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. *0* means there won’t be a time-out. The default value is *30* seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the response timeout for 60 seconds:

```
DES-3028P:4#config authen parameter response_timeout
60
Command: config authen parameter response_timeout 60

Success.

DES-3028P:4#
```

config authen parameter attempt

Purpose	Used to configure the maximum number of times the Switch will accept authentication attempts.
Syntax	**config authen parameter attempt <int 1-255>**
Description	This command 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	*parameter attempt <int 1-255>* – Set the maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.

config authen parameter attempt

Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the maximum number of authentication attempts at 5:

```
DES-3028P:4#config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DES-3028P:4#
```

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-3028P:4#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts        : 5

DES-3028P:4#
```

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 on the normal user level, to become promoted to the administrator level. After logging on to the Switch users will have only user level privileges. To gain access to administrator level privileges, the user will enter this command and will have to enter an authentication password. Possible authentication methods for this function include TACACS, XTACACS, TACACS+, RADIUS, user defined server groups, local enable (local account on the Switch), or no

enable admin

	authentication (*none*). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host which has the username “enable”, and a password configured by the administrator that will support the “enable” function. This function becomes inoperable when the authentication policy is disabled.
Parameters	None.
Restrictions	None.

Example usage:

To enable administrator privileges on the Switch:

```
DES-3028P:4#enable admin
Password: ******

DES-3028P:4#
```

config admin local_enable

Purpose	Used to configure the local enable password for administrator level privileges.
Syntax	**config admin local_enable**
Description	This command 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	*<password 15>* – After entering this command, the user will be prompted to enter the old password, then a new password in an alphanumeric string of no more than 15 characters, and finally prompted to enter the new password again for confirmation. See the example below.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the password for the “local_enable” authentication method.

```
DES-3028P:4#config admin local_enable
Command: config admin local_enable

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

DES-3028P:4#
```

31

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-lever 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]
show ssh server	
config ssh user	<username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>] | password | publickey]
show ssh user authmode	
config ssh algorithm	[3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm	
config ssh regenerate hostkey	

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-level users can issue this command.

Usage example:

To enable SSH:

```
DES-3028P:4#enable ssh
Command: enable ssh

Success.

DES-3028P:4#
```

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-level users can issue this command.

Usage example:

To disable SSH:

```
DES-3028P:4# disable ssh
Command: disable ssh

Success.

DES-3028P:4#
```

config ssh authmode

Purpose	Used to configure the SSH authentication mode setting.
Syntax	**config ssh authmode [password | publickey | hostbased] [enable | disable]**
Description	This command will allow users to configure the SSH authentication mode for users attempting to access the Switch.

config ssh authmode

Parameters	*password* – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the Switch. *publickey* – This parameter may be chosen if the administrator wishes to use a publickey configuration set on a SSH server, for authentication. *hostbased* – This parameter may be chosen if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. *[enable | disable]* – This allows users to enable or disable SSH authentication on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DES-3028P:4#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

DES-3028P:4#
```

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-3028P:4#show ssh authmode
Command: show ssh authmode

The SSH authmode:
Password       : Enabled
Publickey      : Enabled
Hostbased      : Enabled

DES-3028P:4#
```

config ssh server

Purpose	Used to configure the SSH server.
Syntax	**config ssh server {maxsession <int 1-8> | timeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]**

config ssh server

Description	This command allows users to configure the SSH server.
Parameters	*maxsession <int 1-8>* – Allows the user to set the number of users that may simultaneously access the Switch. The default setting is 8. *contimeout <sec 120-600>* – Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default is 120 seconds. *authfail <int 2-20>* – Allows the administrator to set the maximum number of attempts that a user may try to logon utilizing SSH authentication. After the maximum number of attempts is exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. *rekey [10min* | *30min* | *60min* | *never]* – Sets the time period that the Switch will change the security shell encryptions.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To configure the SSH server:

```
DES-3028P:4# config ssh server maxsession 2 contimeout
300 authfail 2
Command: config ssh server maxsession 2 contimeout 300
authfail 2

Success.

DES-3028P:4#
```

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-3028P:4# show ssh server
Command: show ssh server

The SSH server configuration
max Session                 : 8
Connection timeout          : 300
Authfail attempts           : 2
Rekey timeout               : never
port                        : 22

DES-3028P:4#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	**config ssh user <username 15> authmode [hostbased [hostname <domain_name 32>] [hostname_IP <domain_name 32> <ipaddr>] | password | publickey]**
Description	This command allows users to configure the SSH user authentication method.
Parameters	*<username 15>* – Enter a username of no more than 15 characters to identify the SSH user. *authmode* – Specifies the authentication mode of the SSH user wishing to log on to the Switch. The administrator may choose between: *hostbased* – This parameter should be chosen if the user wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. *hostname <domain_name 32>* – Enter an alphanumeric string of up to 32 characters identifying the remote SSH user. *hostname_IP <domain_name 32> <ipaddr>* – Enter the hostname and the corresponding IP address of the SSH user. *password* – This parameter should be chosen to use an administrator defined password for authentication. Upon entry of this command, the Switch will prompt the user for a password, and then to retype the password for confirmation. *publickey* – This parameter should be chosen to use the publickey on a SSH server for authentication.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the SSH user:

```
DES-3028P:4# config ssh user Trinity authmode
password
Command: config ssh user Trinity authmode password

Success.

DES-3028P:4#
```

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	None.

Example usage:

To display the SSH user:

```
DES-3028P:4#show ssh user authmode
Command: show ssh user authmode

```

```
Current Accounts:
UserName       Authentication         Host Name        Host IP
-----------    -----------------    ---------------    --------
Trinity           Password

DES-3028P:4#
```

Note: To configure the SSH user, the administrator must create a user account on the Switch. For information concerning configuring a user account, please see the section of this manual entitled **Basic Switch Commands** and then the command, **create account**.

config ssh algorithm	
Purpose	Used to configure the SSH algorithm.
Syntax	**config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]**
Description	This command allows users to configure the desired type of SSH algorithm used for authentication encryption.
Parameters	*3DES* – This parameter will enable or disable the Triple_Data Encryption Standard encryption algorithm. *AES128* – This parameter will enable or disable the Advanced Encryption Standard AES128 encryption algorithm. *AES192* – This parameter will enable or disable the Advanced Encryption Standard AES192 encryption algorithm. *AES256* – This parameter will enable or disable the Advanced Encryption Standard AES256 encryption algorithm. *arcfour* – This parameter will enable or disable the Arcfour encryption algorithm. *blowfish* – This parameter will enable or disable the Blowfish encryption algorithm. *cast128* – This parameter will enable or disable the Cast128 encryption algorithm. *twofish128* – This parameter will enable or disable the twofish128 encryption algorithm. *twofish192* – This parameter will enable or disable the twofish192 encryption algorithm. *MD5* – This parameter will enable or disable the MD5 Message Digest encryption algorithm. *SHA1* – This parameter will enable or disable the Secure Hash Algorithm encryption. *RSA* – This parameter will enable or disable the RSA encryption algorithm. *DSA* – This parameter will enable or disable the Digital Signature Algorithm encryption. *[enable* | *disable]* – This allows the user to enable or disable algorithms entered in this command, on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To configure SSH algorithm:

```
DES-3028P:4# config ssh algorithm Blowfish enable
Command: config ssh algorithm Blowfish enable

Success.

DES-3028P:4#
```

show ssh algorithm

Purpose	Used to display the SSH algorithm setting.
Syntax	**show ssh algorithm**
Description	This command will display the current SSH algorithm setting status.
Parameters	None.
Restrictions	None.

Usage Example:

To display SSH algorithms currently set on the Switch:

```
DES-3028P:4#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
3DES             :Enabled
AES128           :Enabled
AES192           :Enabled
AES256           :Enabled
ARC4             :Enabled
Blowfish         :Enabled
Cast128          :Enabled
Twofish128       :Enabled
Twofish192       :Enabled
Twofish256       :Enabled

Data Integrity Algorithm
MD5               :Enabled
SHA1              :Enabled

Public Key Algorithm
RSA                :Enabled
DSA                :Enabled

DES-3028P:4#
```

32

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	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	*ciphersuite* – A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. *RSA_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. *DHE_DSS_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. *RSA_EXPORT_with_RC4_40_MD5* – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys. 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.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DES-3028P:4#enable ssl
Command: enable ssl

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

DES-3028P:4#
```

NOTE: Enabling SSL on the Switch will enable all ciphersuites. To utilize a particular ciphersuite, the user must eliminate other ciphersuites by using the **disable ssl** command along with the appropriate ciphersuites.

NOTE: Enabling the SSL function on the Switch will disable the port for the web manager (port 80). To log on to the web based manager, the entry of the URL must begin with *https://*. (ex. https://10.90.90.90).

disable ssl

Purpose	To disable the SSL function on the Switch.
Syntax	**disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}**
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	*ciphersuite* - A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: 1. *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. 2. *RSA_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. 3. *DHE_DSS_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. 4. *RSA_EXPORT_with_RC4_40_MD5* – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DES-3028P:4#disable ssl
Command: disable ssl

Success.

DES-3028P:4#
```

To disable ciphersuite *RSA_EXPORT_with_RC4_40_MD5* only:

```
DES-3028P:4#disable ssl ciphersuite
RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite
RSA_EXPORT_with_RC4_40_MD5

Success.

DES-3028P:4#
```

config ssl cachetimeout timeout

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

config ssl cachetimeout timeout

	key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process.
Parameters	*timeout <value 60-86400>* – Enter a timeout value between *60* and *86400* seconds to specify the total time an SSL key exchange ID stays valid before the SSL module will require a new, full SSL negotiation for connection. The default cache timeout is *600* seconds
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the SSL cachetimeout for 7200 seconds:

```
DES-3028P:4#config ssl cachetimeout timeout 7200
Command: config ssl cachetimeout timeout 7200

Success.

DES-3028P:4#
```

show ssl cachetimeout

Purpose	Used to show the SSL cache timeout.
Syntax	**show ssl cachetimeout**
Description	Entering this command will allow 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-3028P:4#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DES-3028P:4#
```

show ssl

Purpose	Used to view the SSL status and the certificate file status on the Switch.
Syntax	**show ssl**
Description	This command is used to view the SSL status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DES-3028P:4#show ssl
Command: show ssl

 SSL Status                                      Disabled
 RSA_WITH_RC4_128_MD5                    0x0004  Enabled
 RSA_WITH_3DES_EDE_CBC_SHA               0x000A  Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA           0x0013  Enabled
 RSA_EXPORT_WITH_RC4_40_MD5              0x0003  Enabled

DES-3028P:4#
```

show ssl certificate

Purpose	Used to view the SSL certificate file status on the Switch.
Syntax	**show ssl certificate**
Description	This command is used to view the SSL certificate file information currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view certificate file information on the Switch:

```
DES-3028P:4# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DES-3028P:4#
```

download ssl certificate

Purpose	Used to download a certificate file for the SSL function on the Switch.
Syntax	**download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>**
Description	This command is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions.
Parameters	*<ipaddr>* – Enter the IP address of the TFTP server. *certfilename <path_filename 64>* – Enter the path and the filename of the certificate file users wish to download. *keyfilename <path_filename 64>* – Enter the path and the filename of the key exchange file users wish to download.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download a certificate file and key file to the Switch:

```
DES-3028P:4#download ssl certificate 10.53.13.94
certfilename c:/cert.der keyfilename c:/pkey.der
Command: download ssl certificate 10.53.13.94
certfilename c:/cert.der keyfilename c:/pkey.der


Certificate Loaded Successfully!


DES-3028P:4#
```

33

D-LINK SINGLE IP MANAGEMENT COMMANDS

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

SIM is an optional feature on the Switch and can easily be enabled or disabled. SIM grouping has no effect on the normal operation of the Switch in the user's network.

There are three classifications for switches using SIM. The **Commander Switch(CS)**, which is the master switch of the group, **Member Switch(MS)**, which is a switch that is recognized by the CS a member of a SIM group, and a **Candidate Switch(CaS)**, which is a switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

A SIM group can only have one Commander Switch(CS).

All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

A SIM group accepts one Commander Switch (numbered 0) and up to 32 switches (numbered 0-31).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.

SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that is more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DES-3028/28G/28P/52/52P 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-3028/28G/28P/52/52P, 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-3028/28G/28P/52/52P Switches may join the group by either an automatic method or by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send back to the administrator.

When a CS becomes a MS, it automatically becomes a member of the first SNMP community (includes read/write and read only) to which the CS belongs. 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 DES-3028/28G/28P/52/52P Switches have 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-3028P:4#enable sim
Command: enable sim

Success.

DES-3028P:4#
```

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-3028P:4#disable sim
Command: disable sim

Success.

DES-3028P:4#
```

show sim

Purpose	Used to view the current information regarding the SIM group on the Switch.
Syntax	**show sim {[candidates {<candidate_id 1-100>} | members {<member_id 1-32>} | group {commander_mac <macaddr>}] | neighbor]}**
Description	This command will display the current information regarding the SIM group on the Switch, including the following: SIM Version – Displays the current Single IP Management version on the Switch. Firmware Version – Displays the current Firmware version on the Switch. Device Name – Displays the user-defined device name on the Switch.

show sim	
	MAC Address – Displays the MAC Address of the Switch. Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3). Platform – Switch Description including name and model number. SIM State – Displays the current Single IP Management State of the Switch, whether it be enabled or disabled. Role State – Displays the current role the Switch is taking, including Commander, Member or Candidate. A Stand-alone switch will always have the commander role. Discovery Interval – Time in seconds the Switch will send discovery packets out over the network. Hold time – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.
Parameters	*candidates <candidate_id 1-100>* – Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's ID number, listed from 1 to 100. *members <member_id 1-32>* – Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's id number, listed from 1 to 32. *group {commander_mac <macaddr>}* – Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group. *neighbor* – Entering this parameter will display neighboring devices of the Switch. A SIM neighbor is defined as a switch that is physically connected to the Switch but is not part of the SIM group. This screen will produce the following results: 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-3028P:4#show sim
Command: show sim

SIM Version        : VER-1.61
Firmware Version   : 2.00.B23
Device Name        :
MAC Address        : 00-19-5B-EF-78-B5
Capabilities       : L2
Platform           : DES-3028P L2 Switch
SIM State          : Disabled
Role State         : Candidate
Discovery Interval : 30 sec
Holdtime           : 100 sec

DES-3028P:4#
```

To show the candidate information in summary, if the candidate ID is specified:

```
DES-3028P:4#show sim candidates
Command: show sim candidates

ID   MAC Address      Platform /         Hold     Firmware    Device Name
                      Capability         Time     Version
--- ---------------  ----------------  -------  ----------  -------------
1  00-01-02-03-04-00  DES-3028P L2 Switch   40      2.00.B23    The Man
2  00-55-55-00-55-00  DES-3028P L2 Switch  140      2.00.B23    default master

Total Entries: 2

DES-3028P:4#
```

To show the member information in summary:

```
DES-3028P:4#show sim members
Command: show sim members

ID   MAC Address          Platform /           Hold     Firmware     Device Name
                          Capability           Time     Version
--- ----------------- -----------------------   ----     ---------    ----------------
1    00-01-02-03-04-00    DES-3028P L2 Switch     40       2.00.B23      The Man
2    00-55-55-00-55-00    DES-3028P L2 Switch     140      2.00.B23      default master

Total Entries: 2

DES-3028P:4#
```

To show other groups information in summary, if group is specified:

```
DES-3028P:4#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address        Platform /          Hold       Firmware    Device Name
                       Capability          Time       Version
--- ---------------- ------------------   -----      ---------    ----------------
*1  00-01-02-03-04-00   DES-3028P L2 Switch    40        2.00.B23      Trinity
 2  00-55-55-00-55-00   DES-3028P L2 Switch    140       2.00.B23      default master

SIM Group Name : SIM2

ID  MAC Address        Platform /           Hold       Firmware     Device Nam
                       Capability           Time       Version
---  -------------- ----------------       ------     ---------     ----------------
*1  00-01-02-03-04-00   DES-3028P L2 Switch    40       1.00.B23        Neo
 2  00-55-55-00-55-00   DES-3028P L2 Switch    140      1.00.B23        default master

'*' means commander switch.

DES-3028P:4#
```

Example usage:

To view SIM neighbors:

```
DES-3028P:4#show sim neighbor
Command: show sim neighbor

Neighbor Info Table

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

Total Entries: 3

DES-3028P:4#
```

reconfig

Purpose	Used to connect to a member switch, through the commander switch, using Telnet.
Syntax	**reconfig {member_id <value 1-32> | exit}**
Description	This command is used to reconnect to a member switch using Telnet.
Parameters	*member_id <value 1-32>* – Select the ID number of the member switch to configure. *exit* – This command is used to exit from managing the member switch and will return to managing the commander switch.

reconfig

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-3028P:4#reconfig  member_id 2
Command: reconfig  member_id 2

DES-3028P:4#
```

config sim_group

Purpose	Used to add candidates and delete members from the SIM group.
Syntax	**config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]**
Description	This command is used to add candidates and delete members from the SIM group by ID number.
Parameters	*add <candidate_id 1-100> <password>* – Use this parameter to change a candidate switch (CaS) to a member switch (MS) of a SIM group. The CaS may be defined by its ID number and a password (if necessary). *delete <member_id 1-32>* – Use this parameter to delete a member switch of a SIM group. The member switch should be defined by ID number.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a member:

```
DES-3028P:4#config sim_group add 2
Command: config sim_group add 2

Please wait for ACK...
GM Config Success !!!

Success.

DES-3028P:4#
```

To delete a member:

```
DES-3028P:4# config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK...
Success.

DES-3028P:4#
```

config sim

Purpose	Used to configure role parameters for the SIM protocol on the Switch.
Syntax	**config sim [[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>}]**
Description	This command is used to configure parameters of switches of the SIM.
Parameters	*commander* – Use this parameter to configure the commander switch (CS) for the following parameters: *candidate* – Used to change the role of a CS (commander) to a CaS (candidate). ▪ *dp_interval <30-90>* – The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to the CS will include information about other switches connected to it. (Ex. MS, CaS). The user may set the *dp_interval* from 30 to 90 seconds. ▪ *hold time <100-255>* – Using this parameter, the user may set the time, in seconds, the Switch will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 255 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To change the time interval of the discovery protocol:

```
DES-3028P:4# config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DES-3028P:4#
```

To change the hold time of the discovery protocol:

```
DES-3028P:4# config sim hold_time 120
Command: config sim hold_time 120

Success.

DES-3028P:4#
```

To transfer the CS (commander) to be a CaS (candidate):

```
DES-3028P:4# config sim candidate
Command: config sim candidate

Success.

DES-3028P:4#
```

To transfer the Switch to be a CS:

```
DES-3028P:4# config sim commander
Command: config sim commander

Success.

DES-3028P:4#
```

To update the name of a group:

```
DES-3028P:4#  config  sim  commander  group_name
Trinity
Command: config sim commander group_name Trinity

Success.

DES-3028P:4#
```

download sim

Purpose	Used to download firmware or configuration file to an indicated device.
Syntax	**download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {members <mslist 1-32> | all}**
Description	This command will download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	*firmware* – Specify this parameter to download firmware to members of a SIM group. *configuration* – Specify this parameter to download a switch configuration to members of a SIM group. *<ipaddr>* – Enter the IP address of the TFTP server. *<path_filename>* – Enter the path and the filename of the firmware or switch on the TFTP server. *members* – Enter this parameter to specify the members to which the user prefers to download firmware or switch configuration files. The user may specify a member or members by adding one of the following: ▪ *<mslist>* – Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration. ▪ *all* – 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-3028P:4#download sim_ms firmware_from_tftp 10.53.13.94
c:/des3028.had all
```

```
Command: download sim_ms firmware_from_tftp 10.53.13.94
c:/des3028.had all

This device is updating firmware.  Please wait several minutes...

Download Status :

ID    MAC Address         Result
---   ----------------   ---------------
  1   00-36-28-10-35-00   Success



DES-3028P:4#
```

To download configuration files:

```
DES-3028P:4#   download   sim_ms   configuration_from_tftp   10.53.13.94
c:/des3028.txt all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/des3028.txt
all

This device is updating configuration.  Please wait several minutes...

Download Status :

ID    MAC Address         Result
---    ---------------- ---------------
1     00-01-02-03-04-00   Success
2     00-07-06-05-04-03   Success
3     00-07-06-05-04-03   Success

DES-3028P:4#
```

upload sim_ms

Purpose	User to upload a configuration file to a TFTP server from a specified member of a SIM group.
Syntax	**upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> [members <mslist> | all]**
Description	This command will upload a configuration file to a TFTP server from a specified member of a SIM group.
Parameters	*<ipaddr>* – Enter the IP address of the TFTP server to which to upload a configuration file. *<path_filename>* – Enter a user-defined path and file name on the TFTP server to which to upload configuration files. *<member_id 1-32>* – Enter this parameter to specify the member to which to upload a switch configuration file. The user may specify a member or members by adding the ID number of the specified member.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DES-3028P:4#    upload    sim_ms    configuration_to_tftp    10.55.47.1
D:\configuration.txt 1
Command: upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1

This device is upload configuration.  Please wait several minutes ...

Upload Status :

ID   MAC Address             Result
---  -----------------     ------------------------
 1   00-A1-51-34-26-00      Success

DES-3028P:4#
```

35

SMTP COMMANDS

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered using the commands below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events and enhancing security by recording questionable events occurring on the Switch.

The Switch plays four important roles as a client in the functioning of SMTP:

- The server and server virtual port must be correctly configured for this function to work properly. This is accomplished in the **config smtp** command by properly configuring the *server* and *server_port* parameters.
- Mail recipients must be configured on the Switch. This information is sent to the server which then processes the information and then e-mails Switch information to these recipients. Up to 8 e-mail recipients can be configured on the Switch using the **config smtp** command by configuring the *add mail_receiver* and *delete mail_receiver* parameters.
- The administrator can configure the source mail address from which messages are delivered to configured recipients. This can offer more information to the administrator about Switch functions and problems. The personal e-mail can be configured using the **config smtp** command and setting the *self_mail_addr* parameter.
- The Switch can be configured to send out test mail to first ensure that the recipient will receive e-mails from the SMTP server regarding the Switch. To configure this test mail, the SMTP function must first be enabled using the **enable smtp** command and then by entering the **smtp send_testmsg** command. All recipients configured for SMTP will receive a sample test message from the SMTP server, ensuring the reliability of this function.

THE SWITCH WILL SEND OUT E-MAIL TO RECIPIENTS WHEN ONE OR MORE OF THE FOLLOWING EVENTS OCCUR:

- When a cold start occurs on the Switch.
- When a port enters a link down status.
- When a port enters a link up status.
- When SNMP authentication has been denied by the Switch.
- When a switch configuration entry has been saved to the NVRAM by the Switch.
- When an abnormality occurs on TFTP during a firmware download event. This includes *in-process*, *invalid-file*, *violation*, *file-not-found*, *complete* and *time-out* messages from the TFTP server.
- When a system reset occurs on the Switch.

Information within the e-mail from the SMTP server regarding switch events includes:

- The source device name and IP address.
- A timestamp denoting the identity of the SMTP server and the client that sent the message, as well as the time and date of the message received from the Switch. Messages that have been relayed will have timestamps for each relay.
- The event that occurred on the Switch, prompting the e-mail message to be sent.
- When an event is processed by a user, such as save or firmware upgrade, the IP address, MAC address and User Name of the user completing the task will be sent along with the system message of the event occurred.
- When the same event occurs more than once, the second mail message and every repeating mail message following will have the system’s error message placed in the subject line of the mail message.

The following details events occurring during the Delivery Process.

- Urgent mail will have high priority and be immediately dispatched to recipients while normal mail will be placed in a queue for future transmission.
- The maximum number of untransmitted mail messages placed in the queue cannot exceed 30 messages. Any new messages will be discarded if the queue is full.
- If the initial message sent to a mail recipient is not delivered, it will be placed in the waiting queue until its place in the queue has been reached, and then another attempt to transmit the message is made.
- The maximum attempts for delivering mail to recipients is three. Mail message delivery attempts will be tried every five minutes until the maximum number of attempts is reached. Once reached and the message has not been successfully delivered, the message will be dropped and not received by the mail recipient.
- If the Switch shuts down or reboots, mail messages in the waiting queue will be lost.

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

Command	Parameters
enable smtp	
disable smtp	
config smtp	{server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | [add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8>]}
show smtp	
smtp send_testmsg	

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

enable smtp

Purpose	Used to enable the Switch as a SMTP client.
Syntax	**enable smtp**
Description	This command, in conjunction with the **disable smtp command** will enable and disable the Switch as a SMTP client without changing configurations.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SMTP on the Switch.

```
DES-3028:4#enable smtp
Command: enable smtp

Success.

DES-3028:4#
```

disable smtp

Purpose	Used to disable the Switch as a SMTP client.
Syntax	**disable smtp**
Description	This command, in conjunction with the **enable smtp command** will enable and disable the Switch as a SMTP client without changing configurations.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SMTP on the Switch.

```
DES-3028:4#disable smtp
Command: disable smtp

Success.

DES-3028:4#
```

config smtp

Purpose	Used to configure necessary information in setting up the Switch as an SMTP client.
Syntax	**config smtp {server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | [add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8>]}**
Description	This command will allow the user to set the necessary parameters to configure the SMTP server and mail recipients. This command must be completely configured properly for the SMTP function of the switch to correctly operate.
Parameters	*server <ipaddr>* – Enter the IP address of the SMTP server on a remote device. *server_port <tcp_port_number 1-65535>* – Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is 25. *self_mail_addr <mail addr 64>* – Enter the e-mail address from which mail messages will be sent. This address will be the from address on the e-mail message sent to a recipient. Only one self mail address can be configured for this Switch. This string can be no more that 64 alphanumeric characters. *add mail_receiver <mail_addr 64>* – Choose this parameter to add mail recipients to receive e-mail messages from the Switch. Up to 8 e-mail addresses can be added per Switch. *delete mail_receiver <index 1-8>* – Choose this parameter to delete mail recipients from the configured list receiving e-mail messages from the Switch. Up to 8 e-mail addresses can be added per Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the SMTP settings:

```
DES-3028:4#config smtp server 166.99.66.33 server_port 25 add
mail receiver darren_tremblett@nhl.com
Command: config smtp server 166.99.66.33 server_port 25 add
mail receiver darren_tremblett@nhl.com


Success.


DES-3028:4#
```

show smtp

Purpose	Used to view configured parameters for the SMTP function on the Switch.
Syntax	**show smtp**
Description	This command will display parameters configured for SMTP on the Switch, including server information, mail recipients and the current running status of SMTP on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the SMTP parameters currently configured on the Switch:

```
DES-3028:4#show smtp
Command: show smtp

smtp status: Enabled
smtp server address : 166.99.66.33
smtp server port : 25
self mail address: smtp@30XX.dev

Index                Mail Receiver Address
--------             ---------------------------------
1                    darren_tremblett@nhl.com
2                    dave@yeehaw.com
3                    administrator@dlink.com
4                    fattony@themob.com
5
6
7
8

DES-3026:4#
```

smtp send_testmsg

Purpose	Used to send a test message to mail recipients configured on the Switch.
Syntax	**smtp send_testmsg**
Description	This command is used to send test messages to all mail recipients configured on the Switch, thus testing the configurations set and the reliability of the SMTP server.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To send a test mail message to all configured mail recipients.

```
DES-3028:4# smtp send_testmsg
Command: smtp send_testmsg

Subject: This is a SMTP test.
Content: Hello everybody!!

Sending mail, please wait…

Success.

DES-3028:4#
```

35

POE COMMANDS

DES-3028P and the DES-3052P support Power over Ethernet (PoE) as defined by the IEEE 802.3af specification. Ports 1-24/1-48 supply 48 VDC power to PDs over Category 5 or Category 3 UTP Ethernet cables. The DES-3028P and the DES-3052P follow the standard PSE pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. The DES-3028P and the DES-3052P works with all D-Link 802.3af capable devices.

The DES-3028P and the DES-3052P include the following PoE features:

The auto-discovery feature recognizes the connection of a PD (Powered Device) and automatically sends power to it.

The auto-disable feature will occur under two conditions: first, if the total power consumption exceeds the system power limit; and second, if the per port power consumption exceeds the per port power limit.

The active circuit protection feature automatically disables the port if there is a short. Other ports will remain active.

PDs receive power according to the following classification:

Class	Max power used by PD
0	0.44 to 12.95W
1	0.44 to 3.84W
2	3.84 to 6.49W
3	6.49 to 12.95W

PSE provides power according to the following classification:

Class	Max power provided by PSE
0	15.4W
1	4.0W
2	7.0W
3	15.4W

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	{power_limit <value 37-185> | power_disconnect_method [deny_next_port | deny_low_priority_port]}
config poe ports	[all | <portlist>] {state [enable | disable] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-16800>]}
show poe	[system | ports {<portlist>}]

NOTE: The maximum PoE power limit for the DES-3028P is 185W and the maximum PoE power limit for the DES-3052P is 370W.

Each command is listed in detail in the following sections.

config poe system	
Purpose	Used to configure the parameters for the whole PoE system.
Syntax	**config poe system {power_limit <value 37-185> | power_disconnect_method [deny_next_port |**

config poe system

	deny_low_priority_port}
Description	Allows the user to configure the parameters for the whole PoE system.
Parameters	*power_limit* – The power limit parameter allows the user to configure the power budget of whole PoE system. The minimum setting is 37 W and the maximum is 370W (depending on the power supplier's capability). Default setting is 370 W. *power_disconnect_method* – This parameter is used to configure the power management disconnection method. When the total consumed power exceeds the power budget, the PoE controller initiates a port disconnection to prevent overloading the power supply. The controller uses one of the following two ways to implement the disconnection: *deny_next_port* – After the power budget has been exceeded, the next port attempting to power up is denied, regardless of its priority. *deny_low_priority_port* – After the power budget has been exceeded, the next port attempting to power up, causes the port with the lowest priority to shut down (to allow high-priority ports to power up). The default setting is *deny_next_port*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config the PoE System on the Switch:

```
DES-3028P:4#config poe system power_limit 185
power_disconnect_method deny_next_port
Command: config poe system power_limit 185
power_disconnect_method deny_next_port

Success.

DES-3028P:4#
```

config poe ports

Purpose	Used to configure the PoE port settings.
Syntax	**config poe ports [all | <portlist>] {state [enable | disable] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-16800>]}**
Description	The **config poe ports** command is used to configure the PoE port settings.
Parameters	*<portlist>* – Specifies a range of ports to be configured or all the ports. *all* – Specifies that all ports on the Switch will be configured for PoE. *state* – Enables or disables the PoE function on the Switch. *priority* – Setting the port priority affects power-up order and shutdown order. **Power-up order**: When the Switch powers-up or reboots, the ports are powered up according to their priority (*critical* first, then *high* and finally *low*). **Shutdown order**: When the power limit has been exceeded, the ports will shut down according to their

config poe ports

	priority if the power disconnect method is set to *deny_ low_priority_port.* *critical* – Specifying this parameter will nominate these ports has having the highest priority for all configured PoE ports. These ports will be the first ports to receive power and the last to disconnect power. *high* – Specifying this parameter will nominate these ports as having the second highest priority for receiving power and shutting down power. *low* – Specifying this parameter will nominate these ports as having the lowest priority for receiving and shutting down power. These ports will be the first ports to have their power disconnected if the *power_disconnect_method* chosen in the **config poe system** command is *deny_low_priority_port*. *power_limit* – Allows the user to configure the per-port power limit. If a port exceeds its power limit, the PoE system will shut down that port. The minimum user-Defined setting is 1000mW and maximum is 16800mW. The default setting is 15400mW. The user may also choose to define a power class by which to set the power limit, based on the PSE table at the beginning of this section. *class_0* – Choosing this class will set the maximum port limit at 15.4W. *class_1* – Choosing this class will set the maximum port limit at 4.0W. *class_2* – Choosing this class will set the maximum port limit at 7.0W. *class_3* – Choosing this class will set the maximum port limit at 15.4.0W. *user_define* – Choosing this parameter will allow the user to set a power limit between 1000 and 16800mW with a default value of 15400mW.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config the Switch’s ports for PoE:

```
DES-3028P:4#config poe ports 1-3 state enable priority critical
power_limit class_0
Command: config poe ports 1-3 state enable priority critical
power_limit class_0


Power limit has been set to 15400mW(Class 0 PD upper power limit
12.95W + power loss on cable).
Success.


DES-3028P:4#
```

show poe system

Purpose	Used to display the setting and actual values of the whole PoE system.
Syntax	**show poe [system | ports {<portlist>}]**
Description	Display the settings, actual values and port configuration of the whole PoE system.

show poe system	
Parameters	*system* – Choosing this parameter will display the system settings for PoE, such as switch power limit, consumption, remaining useable power and the power disconnection method. *ports* – Choosing this parameter will display the settings for PoE on a port-by-port basis. *<portlist>* – Enter a port or range of ports to be displayed for their PoE settings.
Restrictions	None.

Example usage:

To display the power settings for the switch system:

```
DES-3028P:4#show poe system
Command: show poe system

PoE System Information
---------------------------------------------------
Power Limit                : 185(watts)
Power Consumption          : 0(watts)
Power Remained             : 185(watts)
Power Disconnection Method : Deny Next 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.

DES-3028P:4#
```

Example usage:

To display the power settings for the switch's ports

```
DES-3028P:4#show poe ports
Command: show poe ports
Port   State     Priority     Power Limit(mW)
       Class     Power(mW)    Voltage(decivolt)    Current(mA)
       Status
==============================================================
1      Enabled   Low         15400(User Defined)
       0         0           0                      0
       Off  : Interim state during line detection
2      Enabled   Low         15400(User Defined)
       0         0           0                      0
       Off  : Interim state during line detection
3      Enabled   Low         15400(User Defined)
       0         0           0                      0
       Off  : Interim state during line detection
4      Enabled   Low         15400(User Defined)
       0         0           0                      0
       Off  : Interim state during line detection
5      Enabled   Low         15400(User Defined)
       0         0           0                      0
       Off  : Interim state during line detection

DES-3028P:4#
```

34

CABLE DIAGNOSTICS COMMANDS

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

Command	Parameters
cable_diag ports	[<portlist>| all]

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

cable_diag ports	
Purpose	Used to test the copper cable. If there is an error on the cable, it can determine the type of error and the position where the error occurred.
Syntax	**cable_diag ports [<portlist>|all]**
Description	For FE port, two pairs of cable will be diagnosed. The type of cable error can be open and short. Open means that the cable in the error pair does not have a connection at the specified position. Short means that the cables in the error pair has a short problem at the specified position. When a port is in link-up status, the test will obtain the distance of the cable. Since the status is link-up, the cable will not have the short or open problem. When a port is in link-down status, the link-down may be caused by many factors. When the port has a normal cable connection, but the remote partner is powered off, the cable diagnosis can still diagnose the health of the cable as if the remote partner is powered on. When the port does not have any cable connection, the result of the test will indicate no cable. The test will detect the type of error and the position where the error occurs. Note that this test will consume a low number of packets. Since this test is for copper cable, the port with fiber cable will be skipped from the test. Some phy chips can’t support Cable Diagnostic function, and it will display at the result.
Parameters	*<portlist>* – Specifies a range of ports to be tested. *all* – All ports
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To test the cable on specific ports:

```
DES-3028P:4#cable_diag ports 1-3,10
Command: cable_diag ports 1-3,10
Perform Cable Diagnostics ...

 Port   Type      Link Status    Test Result         Cable Length (M)
 ----  -------  --------------  -----------------    ---------------
  1      FE       Link Down     No Cable                     -
  2      FE       Link Down     No Cable                     -
  3      FE       Link Up       OK                           49
  10     FE       Link Down     No Cable                     -

DES-3028P:4#
```

35

DHCP LOCAL RELAY COMMANDS

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

Command	Parameters
config dhcp_local _relay	vlan[<vlan_name 32> | vlanid <vidlist>] state [enable | disable]
enable dhcp_local _relay	
disable dhcp _local_relay	
show dhcp _local_relay	

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

config dhcp_local_relay vlan	
Purpose	Used to enable/disable DHCP local relay function to vlan.
Syntax	**config dhcp_local_relay vlan [<vlan_name 32>| vlanid <vidlist>] state [enable | disable]**
Description	The config dhcp_local_relay vlan command is used to enable /disable DHCP local relay function for specified vlan. When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed in broadcast way without change of the source MAC address and gateway address. DHCP option 82 will be automatically added.
Parameters	<*vlan_name 32*> – The name of the VLAN to be enabled DHCP local relay. <*vidlist*> – Specifies a range of VLAN IDs to be configured. *state* – Enable or disable DHCP local relay for specified vlan.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable DHCP local relay for the default vlan:

```
DES-3028P:4#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DES-3028P:4#
```

enable dhcp_local_relay	
Purpose	Used to enable the DHCP local relay function on the switch.
Syntax	**enable dhcp_local_relay**
Description	The enable dhcp_local _relay command globally enables the DHCP local relay function on the switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable DHCP local relay function:

```
DES-3028P:4#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DES-3028P:4#
```

disable dhcp_local_relay

Purpose	Used to disable the DHCP local relay function on the switch.
Syntax	**disable dhcp_local_relay**
Description	The disable dhcp_local_relay command globally disables the DHCP local relay function on the switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable DHCP local relay function:

```
DES-3028P:4#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DES-3028P:4#
```

show dhcp_local_relay

Purpose	Used to display the current DHCP local relay configuration.
Syntax	**show dhcp_local_relay**
Description	The show dhcp_local_relay command displays the current DHCP local relay configuration.
Parameters	None.
Restrictions	None.

Example usage:

To show DHCP local relay function:

```
DES-3028P:4# show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status    : Disabled
DHCP/BOOTP Local Relay VLAN List : 1,3-4

DES-3028P:4#
```

36

GRATUITOUS ARP COMMANDS

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

Command	Parameters
config gratuitous_arp send ipif_status_up	[enable | disable]
config gratuitous_arp send dup_ip_detected	[enable|disable]
config gratuitous_arp learning	[enable|disable]
enable gratuitous_arp	{ipif <ipif_name 12>} {trap |log }
disable gratuitous_arp	{ipif <ipif_name 12>} {trap |log}
config gratuitous_arp send periodically ipif	<ipif_name 12> interval <value 0-65535>
show gratuitous_arp	{ipif <ipif_name 12>}

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

config gratuitous_arp send ipif_status_up

Purpose	Used to enable/disable send gratuitous ARP request while the IP interface status is up.
Syntax	**config gratuitous_arp send ipif_status_up [enable | disable]**
Description	The command is used to enable/disable sending of gratuitous ARP request packet while IPIF interface is up. This is used to automatically announce the interface’s IP address to other nodes. By default, the state is enabled, and only one gratuitous ARP packet will be broadcast.
Parameters	*enable* – Enable sending of gratuitous ARP when IPIF status is up. *disable* – Disable sending of gratuitous ARP when IPIF status is up.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable a gratuitous ARP request:

```
DES-3028P:4#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DES-3028P:4#
```

config gratuitous_arp send duplicate_ip_detected

Purpose	Used to enable/disable the sending of gratuitous ARP requests while duplicate IP addresses are detected
Syntax	**config gratuitous_arp send duplicate_ip_detected [enable|disable]**
Description	The command is used to enable/disable sending of gratuitous ARP request packets while duplicate IPs are detected. By default, the state is

config gratuitous_arp send duplicate_ip_detected

	enabled. For this command, the duplicate IP detected means that the system has received an ARP request packet that was sent by an IP address that matched the system's own IP address. In this case, the system knows that somebody out there uses an IP address that is conflicting 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	*enable* – Enable sending of gratuitous ARP when duplicate IP is detected. *disable* – Disable sending of gratuitous ARP when duplicate IP is detected.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable gratuitous ARP request when a duplicate IP is detected:

```
DES-3028P:4#config gratuitous_arp duplicate_ip_detected enable
Command: config gratuitous_arp duplicate_ip_detected enable

Success.

DES-3028P:4#
```

config gratuitous_arp learning

Purpose	Used to enable/disable learning of ARP entries in ARP cache based on the received gratuitous ARP packets.
Syntax	**config gratuitous_arp learning [enable|disable]**
Description	Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. The command is used to enable/disable learning of ARP entry in ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for. Note that, with the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet. By default, the state is Enabled.
Parameters	*enable* – Enable learning of ARP entries based on the received gratuitous ARP packet. *disable* – Disable learning of ARP entry based on the received gratuitous ARP packet.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable learning of ARP entries based on the received gratuitous ARP packets:

```
DES-3028P:4# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DES-3028P:4#
```

config gratuitous_arp periodical_send

Purpose	Used to configure the interval for periodical sending of gratuitous ARP request packets.
Syntax	**config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>**
Description	This command is used to configure the interval for periodical sending of gratuitous ARP request packets. By default, the interval is 0.
Parameters	*<ipif_name 12>* – Interface name of L3 interface. *<value 0-65535>* – Periodically send gratuitous ARP interval time in seconds. 0- means it will not send gratuitous ARP periodically.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure gratuitous ARP intervals for the IPIF System:

```
DES-3028P:4#config  gratuitous_arp  send  periodically  ipif  System
interval 5
Command:  config  gratuitous_arp  send  periodically  ipif  System
interval 5

Success.

DES-3028P:4#
```

enable gratuitous_arp trap and log

Purpose	Used to enable the gratuitous ARP trap and log.
Syntax	**enable gratuitous_arp {ipif <ipif_name 12>} {trap |log}**
Description	The command is used to enable gratuitous ARP trap and log states. The switch can trap and log the IP conflict event to inform the administrator. By default, the trap is disabled and event log is enabled.
Parameters	*<ipif_name 12>* – Interface name of L3 interface.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the System's interface gratuitous ARP log and trap:

```
DES-3028P:4#enable gratuitous_arp System trap log
Command: enable gratuitous_arp System trap log

Success.

DES-3028P:4#
```

disable gratuitous_arp trap and log

Purpose	Used to disable the gratuitous ARP trap and log.
Syntax	**disable gratuitous_arp {ipif <ipif_name 12>} {trap |log}**
Description	The command is used to disable the gratuitous ARP trap and log states. The switch can trap and log the IP conflict event to inform the administrator. By default, the trap is disabled and event log is enabled.
Parameters	*<ipif_name 12>* – Interface name of L3 interface.

disable gratuitous_arp trap and log

Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the System’s interface gratuitous ARP log and trap:

```
DES-3028P:4#disable gratuitous_arp System trap log
Command: disable gratuitous_arp System trap log

Success.

DES-3028P:4#
```

show gratuitous_arp

Purpose	Used to display gratuitous ARP configuration.
Syntax	**show gratuitous_arp {ipif <ipif_name>}**
Description	The show gratuitous_arp command is used to display gratuitous ARP configurations.
Parameters	*<ipif_name 12>* – Interface name of L3 interface.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display gratuitous ARP log and trap states:

```
DES-3028P:4# show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF status up                   : Enabled
Send on Duplicate_IP_Detected            :  Disabled
Gratuitous ARP Learning                  :  Enabled

IP Interface Name : System
Gratuitous ARP Trap/Log                  : Disabled
Gratuitous ARP Log                       : Enabled
Gratuitous ARP Periodical Send Interval  : 5

DES-3028P:4#
```

37

VLAN TRUNKING COMMANDS

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

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

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

enable vlan_trunk

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

Example usage:

To enable the VLAN Trunk:

```
DES-3028P:4#enable vlan_trunk
Command: enable vlan_trunk

Success.

DES-3028P:4#
```

disable vlan_trunk

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

Example usage:

To disable the VLAN Trunk:

```
DES-3028P:4#disable vlan_trunk
Command: disable vlan_trunk

Success.

DES-3028P:4#
```

config vlan_trunk	
Purpose	Used to configure a port as a VLAN trunk port.
Syntax	**config vlan_trunk ports [<portlist>|all] | state [enable|disable]**
Description	This command is used to configure a port as a VLAN trunk port. By default, none of the ports on the Switch are VLAN trunk ports. A VLAN trunk port and a non-VLAN trunk port cannot be grouped as an aggregated link. To change the VLAN trunk setting for an aggregated link, the user must apply the command to the master port. However, this setting will disappear as the aggregated link is destroyed, and the VLAN trunk setting of the individual port will follow the original setting of the port. If the command is applied to link aggregation member port excluding the master, the command will be rejected. The ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as VLAN trunk ports, they are allowed to form an aggregated link. For a VLAN trunk port, the VLANs on which the packets can be by passed will not be advertised by GVRP on that particular port. However, since the traffic on these VLANs are forwarded, this vlan trunk port should participate the MSTP instances corresponding to these VLAN.
Parameters	*<portlist>* – Specifies the list of ports to be configured. *enable* – Specifies that the port is a VLAN trunk port. *disable* – Specifies that the port is not a VLAN trunk port.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a VLAN Trunk port:

```
DES-3028P:4#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DES-3028P:4#
```

To configure a VLAN Trunk port if Port 6 is LA-1 member port; port 7 is LA-2 master port.

```
DES-3028P:4# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Can not operate the member ports of any trunk.

DES-3028P:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DES-3028P:4# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Can not operate the member ports of any trunk.

DES-3028P:4#
```

To configure a VLAN Trunk port if Port 6 is LA-1 member port, port 7 is LA-1 master port.

```
DES-3028P:4# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DES-3028P:4#
```

To configure a VLAN Trunk port if Port 6,7 have the same VLAN configurations before enable VLAN trunking. Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DES-3028P:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DES-3028P:4# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DES-3028P:4#
```

show vlan_trunk

Purpose	Used to display VLAN trunk configuration.
Syntax	**show vlan_trunk**
Description	Shows the VLAN trunk information.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display VLAN Trunk information:

```
DES-3028P:4#show vlan_trunk
Command: show vlan_trunk

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

DES-3028P:4#
```

38

QINQ COMMANDS

The QinQ 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	
config qinq ports	[<portlist>|all] {role [nni | uni] | tpid [<hex 0x0 – 0xffff>}
show qinq ports	{<portlist>}

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

enable qinq

Purpose	This command is used to enable the QinQ mode.
Syntax	**enable qinq**
Description	This command enables QinQ mode. When QinQ is enabled, all network port roles will be NNI port and their outer TPID will be set to 88a8. All existing static VLANs will run as SP-VLAN. All dynamically learned L2 address will be cleared. GVRP and STP need to be disabled manually. If you need to run GVRP on the switch, firstly enable GVRP manually. The default setting of QinQ is disabled
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable QinQ:

```
DES-3028P:4#enable qinq
Command: enable qinq

Success.

DES-3028P:4#
```

disable qinq

Purpose	This command is used to disable the QinQ mode.
Syntax	**disable qinq**
Description	This command disables QinQ mode. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared, GVRP will be disabled. If you need to run GVRP on the switch, firstly enable GVRP manually. All existing SP-VLANs will run as static 1Q VLANs. The default setting of QinQ is disabled
Parameters	None.

disable qinq

Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable QinQ:

```
DES-3028P:4#disable qinq
Command: disable qinq

Success.

DES-3028P:4#
```

show qinq

Purpose	Used to show global qinq
Syntax	**show qinq**
Description	This command is used to show the global QinQ status.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To show global QinQ status:

```
DES-3028P:4#show qinq
Command: show qinq

QinQ Status: Enabled

DES-3028P:4#
```

configure qinq port

Purpose	Used to configure qinq ports.
Syntax	**config qinq ports [<portlist>|all] {role [nni | uni] | tpid <hex 0x0–0xffff>}**
Description	This command used to configure the QinQ VLAN mode for ports, including: The port role in double tag VLAN mode, and port outer TPID. This setting will not be effective when QinQ mode is disabled.
Parameters	*<portlist>* – A range of ports to configure. *role* – Port role in QinQ mode, it can be UNI port or NNI port. *TPID* – Specifies the tpid of the Double VLAN. The default setting is 0x88a8. This switch does not support TPID 0x8810.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure port list 1-4 as NNI port, set outer TPID to 0x88a8:

```
DES-3028P:4# config qinq ports 1-4 role nni tpid 0x88a8
Command: config qinq ports 1-4 role nni tpid 0x88a8

Success.

DES-3028P:4#
```

show qinq ports

Purpose	Used to show global qinq and port’s qinq mode status.
Syntax	**show qinq ports <portlist>**
Description	The command used to show the qinq configuration for a port, including: port role in QinQ mode, port outer TPID, that is applied to the port.
Parameters	*<portlist>* – Specifies a range of ports to be displayed. If no parameter is specified, the system will display all port information.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To show double tagging mode for ports 1-4 of unit 1:

```
DES-3028P:4# DES-3028P:4#show qinq ports 4
Command: show qinq ports 4

Port     Role      TPID
-----    ------    ------
4        Normal    0x8100

Total Entries  : 1

DES-3028P:4#
```

39

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-level users can issue this command.

Example usage:

To enable asymmetric VLANs:

```
DES-3028P:4#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DES-3028P:4#
```

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-level users can issue this command.

Example usage:

To disable asymmetric VLANs:

```
DES-3028P:4#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DES-3028P:4#
```

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-3028P:4#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN: Enabled

DES-3028P:4#
```

40

MLD SNOOPING COMMANDS

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

Command	Parameters
config mld_snooping	[vlan <vlan_name 32> | vlanid <vlanid_list>|all] { node_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | done_timer <sec 1-16711450> | state [enable|disable] | fast_done [enable|disable] }
config mld_snooping mrouter_ports	[<vlan_name 32>| [add|delete]<portlist>
config mld_snooping mrouter_ports_forbidden	[<vlan_name 32>] [add|delete]<portlist>
enable mld_snooping	
disable mld_snooping	
show mld_snooping	{vlan <vlan_name 32>| vlanid <vlanid_list>}
show mld_snooping group	{vlan <vlan_name 32>| vlanid <vlanid_list>}
show mld_snooping mrouter_ports	{vlan <vlan_name 32>| vlanid <vlanid_list>} { [static|dynamic|forbidden]}

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

config mld_snooping

Purpose	Used to configure MLD snooping on the switch.
Syntax	**config mld_snooping [vlan <vlan_name 32>| vlanid <vlanid_list>| |all] { node_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | done_timer <sec 1-16711450> | state [enable|disable] | fast_done [enable|disable] }**
Description	The config mld_snooping 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	*<vlan_name 32>* – The name of the VLAN for which MLD snooping is to be configured. *all* – Specifies that all VLANs will be configured. *node_timeout* – Specifies the amount of time that must pass before a link node is considered to not be a listener anymore. The default is 260 seconds. *router_timeout* – Specifies the maximum amount of time a router will remain in the switch, and can be a listener of a multicast group without the switch receiving a node listener report. The default is 260 seconds. *done_timer* – Specifies the maximum amount of time a group will remain in the switch after receiving a done message from the group without receiving a node listener report. The default setting is 2 seconds. *state* – Allows you to enable or disable the MLD snooping function for

config mld_snooping

	the chosen VLAN. *fast_done* – enable or disable MLD snooping fast_done function.If enable, the membership is immediately removed when the system receives the MLD done message.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

```
To configure the MLD snooping to the default vlan
with node_timeout 250 sec and state enable:DES-
3028P:4#config mld_snooping vlan default
node_timeout 250 state enable
Command: config mld_snooping vlan default
node_timeout 250 state enable


Success.


DES-3028P:4#
```

config mld_snooping mrouter_ports

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

Example usage:

To set up port range 1-10 to be static router ports:

```
DES-3028P:4# config mld_snooping mrouter_ports
default add 1-10
Command: config mld_snooping mrouter_ports default
add 1-10

Success.

DES-3028P:4#
```

config mld_snooping mrouter_ports_forbidden

Purpose	Used to configure ports as forbidden router ports.
Syntax	**config mld_snooping mrouter_ports_forbidden [<vlan_name 32> | vlanid <vlanid >] [add|delete] <portlist>**
Description	The config mld_snooping mrouter_ports_forbidden command allows you to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *add* | *delete* – Specifies to add or delete the router ports. *<portlist>* – Specifies a range of ports to be configured. (UnitID:port number)
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set up port range 1-10 to forbidden router ports:

```
DES-3028P:4#config mld_snooping mrouter_ports_forbidden default add 1-10
Command: config mld_snooping mrouter_ports_forbidden default add 1-10

Success.

DES-3028P:4#
```

enable mld_snooping

Purpose	Used to enable MLD snooping on the switch.
Syntax	**enable mld_snooping**
Description	The enable mld_snooping command allows you to enable MLD snooping on the switch. The switch will forward all multicast traffic to the multicast router, only. Otherwise, the switch forwards all multicast traffic to any IPv6 router.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable MLD snooping on the switch:

```
DES-3028P:4# enable mld_snooping
Command: enable mld_snooping

Success.

DES-3028P:4#
```

disable mld_snooping

Purpose	Used to disable MLD snooping on the switch.
Syntax	**disable mld_snooping**
Description	The disable mld_snooping command disables MLD snooping on the switch. Disabling MLD snooping allows all MLD and IPv6 multicast traffic to flood within a given IPv6 interface by default.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable MLD snooping on the switch:

```
DES-3028P:4# disable mld_snooping
Command: disable mld_snooping

Success.

DES-3028P:4#
```

show mld_snooping

Purpose	Used to show the current status of MLD snooping on the switch.
Syntax	**show mld_snooping {vlan <vlan_name 32> | vlanid <vlanid_list>}**
Description	The show mld_snooping will display the current MLD snooping configuration on the switch.
Parameters	<*vlan_name 32*> – 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 configuration.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To show mld_snooping:

```
DES-3028P:4# show mld_snooping
Command: show mld_snooping

MLD Snooping Global State    : Disabled
Multicast router Only        : Disabled

VLAN  Name                   : default
Query Interval               : 125
Max Response Time            : 10
Robustness Value             : 2
Last Listener Query Interval : 1
Node Timeout                 : 260
Router Timeout               : 260
Done Timer                   : 2
Querier State                : Disabled
Querier Router Behavior      : Non-Querier
State                        : Disabled
Version                      : 2

VLAN  Name                   : vlan2
Query Interval               : 125
Max Response Time            : 10
Robustness Value             : 2
Last Listener Query Interval : 1
Node Timeout                 : 260
Router Timeout               : 260
Done Timer                   : 2
Querier State                : Disabled
Querier Router Behavior      : Non-Querier
State                        : Disabled
Version                      : 1

Total Entries: 2

DES-3028P:4#
```

show mld_snooping group

Purpose	Used to display the current MLD snooping group configuration on the switch.
Syntax	**show mld_snooping group {vlan <vlan_name 32>| vlanid <vlanid_list>}**
Description	The show mld_snooping group displays the current MLD snooping group configuration on the switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which you want to view MLD snooping group configuration information. If no parameter specified, the system will display all current MLD group snooping configuration of the switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To show MLD snooping group:

```
DES-3028P:4#show mld_snooping group
Command: show mld_snooping group

Source/Group     :   2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID    :   default/1
Member Ports     :   1-2
Filter Mode      :   INCLUDE

Source/Group     :   2000::100:10:10:5/FF0E::100:0:0:20
VLAN Name/VID    :   default/1
Member Ports     :   3
Filter Mode      :   EXCLUDE

Source/Group     :   NULL/FF0E::100:0:0:21
VLAN Name/VID    :   default/1
Member Ports     :   4-5
Filter Mode      :   EXCLUDE

DES-3028P:4#
```

show mld_snooping mrouter_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	**show mld_snooping mrouter_ports {vlan <vlan_name 32>| vlanid <vlanid_list>}{static|dynamic|forbidden}**
Description	The show mld_snooping mrouter_ports command displays the currently configured router ports on the switch.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *static* – Displays router ports that have been statically configured. *dynamic* – Displays router ports that have been dynamically configured. *forbidden* – Displays forbidden router ports that have been statically configured. If no parameter specified, the system will display all currently configured router ports on the switch.
Restrictions	None.

Example usage:

To display the router ports:

```
DES-3028P:4# show mld_snooping mrouter_ports
Command: show mld_snooping mrouter_ports

VLAN Name                : default
Static mrouter port      : 1-10
Dynamic mrouter port     :
Forbidden mrouter port   :

VLAN Name                : vlan2
Static mrouter port      :
Dynamic mrouter port     :
Forbidden mrouter port   :

Total Entries : 2

DES-3028P:4#
```

41

IGMP SNOOPING MULTICAST VLAN COMMANDS

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

Command	Parameters
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 32> {[add|delete] [member_port <portlist> | tag_member_port <portlist> | source_port <portlist>] |state [enable | disable] | replace_source_ip [<ipaddr> | none]}
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add <mcast_address_list> | delete [<mcast_address_list> | all]]
show igmp_snooping multicast_vlan_group	{< vlan_name 32> }
delete igmp_snooping multicat_vlan	<vlan_name 32>
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
show igmp_snooping multicast_vlan	{<vlan_name 32>}

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

create igmp_snooping multicast_vlan

Purpose	Used to create a multicast VLAN
Syntax	**create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>**
Description	The create igmp_snooping multicast_vlan command will create a multicast_vlan. Multiple multicast VLAN can be configured. The ISM VLAN being created can not exist in the 1Q VLAN database. Multiple ISM VLAN can be created. The ISM VLAN snooping function co-exist with the 1Q VLAN snooping function.
Parameters	<*vlan_name*> – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters. <*vlanid*> – The VLAN ID of the multicast VLAN to be create. The range is 2-4094
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create IGMP snoop multicast VLAN mv12:

```
DES-3028P:4# create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2

Success.


DES-3028P:4#
```

config igmp_snooping multicast_vlan

Purpose	Used to configure the parameter of the specific multicast VLAN.
Syntax	**config igmp_snooping multicast_vlan <vlan_name 32> {[add|delete] [member_port <portlist>| tag_member_port <portlist> | source_port <portlist>] | state [enable | disable] | replace_source_ip [<ipaddr>|none]}**
Description	The **config igmp_snooping multicast_vlan** command allows you to add a member port, add a tag member port, and add a source port to the port list. The member port will automatically become the untagged member of the multicast VLAN, the tag member port and the source port will automatically become the tagged member of the multicast VLAN. To change the port list, the new port list will replace the previous port list if the add or delete is not specified. The member port list and source port list can not overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN. The multicast VLAN must be created first before configuration.
Parameters	*<vlan_name>* – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters. *member_port <portlist>* – A range of member ports to add to the multicast VLAN. They will become the untagged member port of the ISM VLAN. *tag_member_port <portlist>* – Specifies the tagged member port of the ISM VLAN. *source_port* – A range of source ports to add to the multicast VLAN. *state* - enable or disable multicast VLAN for the chosen VLAN. *replace_source_ip* – With the IGMP snooping function, the IGMP report packet sent by the host will be forwarded to the source port. Before the forwarding of the packet, the source IP address in the join packet needs to replaced by this IP address. If none is specified the source IP address will not be replaced. *none* – Specifies that the source IP address will not be replaced.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure an IGMP snoop multicast VLAN:

```
DES-3028P:4# config igmp_snooping multicast_vlan v1 add member_port
1,3 state enable
Command: config igmp_snooping multicast_vlan v1 add member_port 1,3
state enable

Success.
```

```
DES-3028P:4#
```

config igmp_snooping multicast_vlan_group

Purpose	Used to configure the multicast group which will be learned with the specific multicast VLAN.
Syntax	**<vlan_name 32> [add <mcast_address_list> | delete [<mcast_address_list> | all]]**
Description	Used to configure the multicast group which will be learned with the specific multicast VLAN. There are two cases need to be considered. The join packet will be learned with the multicast VLAN that contain the destination multicast group. If the destination multicast group of the join packet can not be classified into any multicast VLAN that this port belong, then the join packet will be learned with the natural VLAN of the packet. **Note:** The same multicast group can not be overlapped in different multicast VLANs. Multiple multicast groups can be added to a multicast VLAN.
Parameters	*<vlan_name 32>* – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters. *<mcast_address_list>* – The list of multicast groups that will be learned with the specified multicast VLAN. *all* – All multicast groups will be selected from the specified multicast VLAN.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a group to a multicast VLAN:

```
DES-3028P:4#config igmp_snooping multicast_vlan_group v1 add 225.1.1.1
Command: config igmp_snooping multicast_vlan_group v1 add 225.1.1.1

Success.

DES-3028P:4#
```

show igmp_snooping multicast_vlan_group

Purpose	Used to display the multicast groups configured for the specified multicast VLAN.
Syntax	**show igmp_snooping multicast_vlan_group {< vlan_name 32> }**
Description	Used to display the multicast groups configured for the specified multicast VLAN.
Parameters	*<vlan_name 32>* – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters.
Restrictions	None.

Example usage:

To display the multicast groups configured for a multicast VLAN.

```
DES-3028P:4#show multicast_vlan_group v1
Command: show multicast_vlan_group v1

VLAN Name      VLAN ID      From          To
-----------    ---------    ----------    ---------
    v1          100         224.19.62.34  224.19.162.200

DES-3028P:4#
```

delete igmp_snooping multicast_vlan

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

Example usage:

To delete an IGMP snoop multicast VLAN:

```
DES-3028P:4# delete igmp_snooping multicat_vlan v1
Command: delete igmp_snooping multicat_vlan v1

Success.

DES-3028P:4#
```

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. By default, the multicast VLAN is in a disabled state.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable IGMP snoop multicast VLAN:

```
DES-3028P:4# enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DES-3028P:4#
```

disable igmp_snooping multicast_vlan

Purpose	Used to disable the multicast VLAN function.
Syntax	**disable 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. By default, the multicast VLAN is in a disabled state.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable IGMP snoop multicast VLAN:

```
DES-3028P:4#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DES-3028P:4#
```

show igmp_snooping multicast_vlan

Purpose	Used to show the information of multicast VLAN.
Syntax	**show igmp_snooping multicast_vlan {<vlan_name 32>}**
Description	The **show igmp_snooping multicast_vlan** command allows you to show the information of multicast VLAN.
Parameters	*<vlan_name 32>* – The name of the multicast VLAN to be shown.
Restrictions	None.

Example usage:

To display IGMP snoop multicast VLAN:

```
DES-3028P:4# show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

VLAN Name               : mv1
VID                     : 2
Member(Untagged) Ports  : 1,3
Tagged Member Ports     : 2
Source Ports            : 4
Status                  : Enabled
Replace Source IP       : 0.0.0.0

DES-3028P:4#
```

42

LIMITED IP MULTICAST ADDRESS COMMANDS

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

Command	Parameters
create mcast_filter_profile profile_id	<value 1-24> profile_name <name 1-32>
config mcast_filter_profile	[profile_id < value 1-24>| profile_name <name 1-32>] { profile_name <name 1-32> | [add | delete] <mcast_address_list>}
delete mcast_filter_profile	[profile_id [<value 1-24> | all]
delete mcast_filter_profile	profile_name <name 1-32>
show mcast_filter_profile	{ [profile_id <value 1-24>|profile_name <name 1-32>]}
config limited_multicast_addr ports	<portlist> {[add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] }
show limited_multicast_addr ports	{<portlist>}
config max_mcast_group port	<portlist> max_group [<value 1-256>]
show max_mcast_group ports	{ <portlist>}

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

create mcast_filter_profile profile_id

Purpose	This command creates a multicast address profile.
Syntax	**create mcast_filter_profile profile_id <value 1-24> profile_name <name 1-32>**
Description	This command creates a multicast address profile. Multiple ranges of multicast addresses can be defined in the profile.
Parameters	*profile_id* – ID of the profile. Range is 1 to 24. *profile_name* – Provides a meaningful description for the profile
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an mcast filter profile:

```
DES-3028P:4#    create    mcast_filter_profile    profile_id    2
profile_name MOD
Command:  create  mcast_filter_profile  profile_id  2  profile_name
MOD

Success.

DES-3028P:4#
```

config mcast_filter_profile

Purpose	This command configures a multicast addresses profile.
Syntax	**config mcast_filter_profile [profile_id < value 1-24>| profile_name <name>] { profile_name <name> | [add | delete] <mcast_address_list>}**
Description	This command is used to configure the multicast filter profiles.
Parameters	*profile_id* – ID of the profile. *profile_name* – Provides a meaningful description for the profile. <*mcast_address_list*> – List of the multicast addresses to be put in the profile. You can either specify a single multicast IP address or a range of multicast addresses.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure an mcast filter profile:

```
DES-3028P:4#  config  mcast_filter_profile  profile_id  2  add
225.1.1.1 - 225.1.1.1
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 -
225.1.1.1

Success.

DES-3028P:4#
```

delete mcast_filter_profile

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

Example usage:

To delete a multicast address profile:

```
DES-3028P:4# delete mcast_filter_profile profile_id  3
Command: delete mcast_filter_profile profile_id  3

Success.

DES-3028P:4#
```

delete mcast_filter_profile

Purpose	This command deletes a multicast address profile.
Syntax	**delete mcast_filter_profile profile_name <name 1-32>**

delete mcast_filter_profile

Description	This command deletes a multicast address profile.
Parameters	*profile_name* – Name of the profile.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a multicast address profile by name:

```
DES-3028P:4#delete mcast_filter_profile profile_name rg
Command: delete mcast_filter_profile profile_name rg

Success.

DES-3028P:4#
```

show mcast_filter_profile

Purpose	This command displays 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	*profile_id* – ID of the profile. *profile_name* – Name of the profile If not specified, all profiles will be displayed.
Restrictions	None.

Example usage:

To display the mcast filter profile:

```
DES-3028P:4# show mcast_filter_profile
Command: show mcast_filter_profile

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

Total Entries : 2
DES-3028P:4#
```

config limited_multicast_addr ports

Purpose	Used to configure the multicast address filtering function on a port.
Syntax	**config limited_multicast_addr ports <portlist> {[add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] }**
Description	Used to configure the multicast address filtering function on a port. When there are no profiles specified with a port, the limited function is not effective. When the function is configured on a port, it limits the multicast group operated by the IGMP or MLD snooping function and layer 3 function.
Parameters	*<portlist>* – A range of ports to config the multicast address filtering function. *add* – Add a multicast address profile to a port. *delete* – Delete a multicast address profile to a port. *profile_id* – A profile to be added to or deleted from the port.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure ports 1,3 to set the multicast address profile 2:

```
DES-3028P:4# config limited_multicast_addr  ports 1,3  add
profile_id 2
Command: config  limited_multicast_addr   ports  1,3   add
profile_id 2

Success.

DES-3028P:4#
```

show limited multicast address

Purpose	Used to show per-port Limited IP multicast address range.
Syntax	**show limited_multicast_addr { ports <portlist> }**
Description	The show limited multicast address command allows you to show multicast address ranges by ports. When the function is configured on a port, it limits the multicast groups operated by the IGMP or MLD snooping function and layer 3 function.
Parameters	*<portlist>* – A range of ports to show the limited multicast address configuration.
Restrictions	None.

Example usage:

To display the limited multicast address range:

```
DES-3028P:4#show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Max Multicast Filter Group:

Port: 1
Profile Id:
```

```
Port: 3
Profile Id:

DES-3028P:4#
```

config max_mcast_group

Purpose	This command configures the maximum number of multicast groups that a port can join.
Syntax	**config max_mcast_group <portlist> max_group <value 1-256>**
Description	This command configures the maximum number of multicast group that a port can join.
Parameters	*<portlist>* – A range of ports to config the max_mcast_group. *max_group* – Specifies the maximum number of multicast groups. The range is from 1 to 256. 256 is the default setting.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the maximum number of multicast groups that a port can join:

```
DES-3028P:4#config  max_mcast_group  ports  1,  3  max_group
100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DES-3028P:4#
```

show max_mcast_group

Purpose	This command displays the maximum number of multicast groups that a port can join.
Syntax	**show max_mcast_group { <portlist>}**
Description	This command displays the maximum number of multicast groups that a port can join.
Parameters	*<portlist>* – A range of ports to display the maximum number of multicast groups.
Restrictions	None.

Example usage:

To display the max number of multicast groups:

```
DES-3028P:4#show max_mcast_group ports 1
Command: show max_mcast_group ports 1

Max Multicast Filter Group:

 Port     MaxMcastGroup
 -----    -------------
 1        256

DES-3028P:4#
```

43

LLDP COMMANDS

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

Command	Parameters
enable lldp	
disable lldp	
config lldp message_tx_interval	<sec 5 - 32768 >
config lldp message_tx_hold_multiplier	< int 2 - 10 >
config lldp tx_delay	< sec 1 - 8192 >
config lldp reinit_delay	< sec 1 - 10 >
config lldp notification_interval	<sec 5 - 3600 >
config lldp ports	[<portlist>|all] notification [enable | disable]
config lldp ports	[<portlist>|all] admin_status [tx_only | rx_only | tx_and_rx | disable]
config lldp ports	[<portlist>|all] mgt_addr ipv4 <ipaddr> [enable | disable]
config lldp ports	[<portlist>|all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_pvid [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_ protocol_identity[all | { eapol | lacp | gvrp | stp }] [enable | disable]
config lldp ports	config lldp ports [<portlist>|all] dot3_tlvs [all | {mac_phy_configuration_status | link aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]
config lldp forward_message	[enable | disable]
show lldp	
show lldp mgt_addr	{ipv4 <ipaddr>}
show lldp ports	{<portlist>}
show lldp local_ports	{ <portlist>} {mode [brief | normal | detailed]}
show lldp remote_ports	{<portlist>} {mode [brief | normal | detailed]}
show lldp statistics	
show lldp statistics ports	{<portlist>}

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

enable lldp

Purpose	Used to enable LLDP operations on the switch.
Syntax	**enable lldp**
Description	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-level users can issue this command.

Example usage

To enable LLDP:

```
DES-3028P:4# enable lldp
Command: enable lldp

Success.

DES-3028P:4#
```

disable lldp

Purpose	Used to disable LLDP operation on the switch.
Syntax	**disable lldp**
Description	The switch will stop sending and receiving of LLDP advertisement packets.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable LLDP:

```
DES-3028P:4# disable lldp
Command: disable lldp

Success.

DES-3028P:4#
```

config lldp message_tx_interval

Purpose	Used to change the packet transmission interval.
Syntax	**config lldp message_tx_interval <sec 5 - 32768 >**
Description	This interval controls how often active ports retransmit advertisements to their neighbors.
Parameters	*message_tx_interval* – Changes the interval between consecutive

config lldp message_tx_interval

	transmissions of LLDP advertisements on any given port. The range is from 5 to 32768 seconds. The default setting is 30 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the packet transmission interval:

```
DES-3028P:4# config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DES-3028P:4#
```

config lldp message_tx_hold_multiplier

Purpose	This command is used to configure the message hold multiplier.
Syntax	**config lldp message_tx_hold_multiplier < int 2 - 10 >**
Description	This parameter 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	*message_tx_hold_multiplier* – The range is from 2 to 10. The default setting 4.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the multiplier value:

```
DES-3028P:4# config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

DES-3028P:4#
```

config lldp tx_delay

Purpose	Used to change the minimum time (delay-interval) of any LLDP port. It will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The tx_delay defines the minimum interval between the sending of LLDP messages due to constant changes of MIB content.
Syntax	**config lldp tx_delay < sec 1–8192 >**
Description	The LLDP message_tx_interval (transmit interval) must be greater than or equal to (4 x tx_delay interval).
Parameters	*tx_delay* – The range is from 1 second to 8192 seconds. The default setting 2 seconds. NOTE: txDelay should be less than or equal to 0.25 * msgTxInterval
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the delay-interval interval:

```
DES-3028P:4# config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DES-3028P:4#
```

config lldp reinit_delay

Purpose	Change the minimum time of 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	reinit_delay – The range is from 1 second to 10 seconds. The default setting 2 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the re-initialization delay interval:

```
DES-3028P:4# config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DES-3028P:4#
```

config lldp notification_interval

Purpose	Used to configure the timer of the notification interval used to send notifications to configured SNMP trap receiver(s).
Syntax	**config lldp notification_interval <sec 5 - 3600 >**
Description	Globally change the interval between successive LLDP change notifications generated by the switch.
Parameters	*notification_interval* – The range is from 5 second to 3600 seconds. The default setting is 5 seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the notification interval:

```
DES-3028P:4# config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DES-3028P:4#
```

config lldp ports notification	
Purpose	Used to configure each port for sending notifications to configured SNMP trap receiver(s).
Syntax	**config lldp ports [<portlist>|all] notification [enable | disable]**
Description	Enable or disable each port for sending change notifications to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout and information update. And the changed type includes any data update /insert/remove.
Parameters	*<portlist>* – Specified a range of ports to be configured. *all* – To set all ports in the system, you may use the “all” parameter. *notification* – Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To change the port SNMP notification state:

```
DES-3028P:4# config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DES-3028P:4#
```

config lldp admin_status	
Purpose	Used to configure per-port transmit and receive modes.
Syntax	**config lldp ports [<portlist>|all] admin_status [tx_only | rx_only | tx_and_rx | disable]**
Description	These options enable the Switch to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.
Parameters	*<portlist>* – Specified a range of ports to be configured. *all* – To set all ports in the system, you may use the “all” parameter. *admin_status* – To set the 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

config lldp admin_status

	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-level users can issue this command.

Example usage

To configure the port’s transmit and receive mode:

```
DES-3028P:4# config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DES-3028P:4#
```

config mgt_addr

Purpose	Used to enable or disable the port(s) which have been specified for advertising the indicated management address instances.
Syntax	**config lldp ports [<portlist>|all] mgt_addr ipv4 <ipaddr> [enable | disable]**
Description	This command 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>* – Specified a range of ports to be configured. *all* – To set all ports in the system, you may use the “all” parameter. *ipv4* – IP address of IPV4.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable port 1 to port 2 for manage address entries:

```
DES-3028P:4# config lldp ports 1-2 mgt_addr ipv4 192.168.254.10
enable
Command:  config  lldp  ports  1-2  mgt_addr  ipv4  192.168.254.10
enable

Success

DES-3028P:4#
```

config lldp basic_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of the optional TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]**

config lldp basic_tlvs

Description	An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, Time to Live TLV). The mandatory type can not be disabled. There are also four data types which can be optionally selected. They are port_description, system_name, system_description, and system_capability.
Parameters	*<portlist>* – Specified a range of ports to be configured. *all* – To set all ports in the system, you may use the “all” parameter. *port_description* – This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled. *system_name* – This TLV optional data type indicates that the LLDP agent should transmit 'System Name TLV'. The default state is disabled. *system_description* – This TLV optional data type indicates that the LLDP agent should transmit 'System Description TLV'. The default state is disabled. *system_capabilities* – This TLV optional data type indicates that the LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router functions, and whether the provided functions are currently enabled. The default state is disabled.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the Switch to exclude the system name TLV from outbound LLDP advertisements on all ports:

```
DES-3028P:4#  config  lldp  ports  all  basic_tlvs  system_name
enable
Command: config lldp ports all basic_tlvs system_name enable


Success.


DES-3028P:4#
```

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 come 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	*<portlist>* – Specified a range of ports to be configured. *all* – To set all ports in the system, you may use the “all” parameter. *dot1_tlv_pvid* – This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disable.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the vlan name TLV from the outbound LLDP advertisements for all ports:

```
DES-3028P:4# config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DES-3028P:4#
```

config lldp dot1_tlv_vlan_name

Purpose	Used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 Organizational VLAN name TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable]**
Description	This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs those enabled VLAN IDs will be advertised.
Parameters	*<portlist>* – Specified a range of ports to be configured. *all* – To set all ports in the system, you may use the "all" parameter. *dot1_tlv_vlan_name* – This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs those enabled VLAN IDs will be advertised. The default state is disable.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DES-3028P:4# config lldp ports all dot1_tlv_vlan_name vlanid 1-
3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3
enable

Success.

DES-3028P:4#
```

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 organization protocol identity TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_ protocol_identity [all | {eapol | lacp | gvrp | stp }] [enable | disable]**
Description	This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations which are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port

config lldp dot1_tlv_protocol_identity

	and it is enabled to be advertised, then this protocol identity will be advertised.
Parameters	*<portlist>* – Specified a range of ports to be configured. *all* – To set all ports in the system, you may use the “all” parameter. *dot1_tlv_ protocol_identity* – This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised. The default state is disable.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DES-3028P:4# config lldp ports all dot1_tlv_protocol_identity
all enable
Command: config lldp ports all dot1_tlv_protocol_identity all
enable


Success.


DES-3028P:4#
```

config lldp dot3_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.3 organization specific TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] dot3_tlvs [all | {mac_phy_configuration_status | link aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]**
Description	Each Specific TLV in this extension can be enabled individually.
Parameters	*<portlist>* – Specified a range of ports to be configured. *all* – To set all ports in the system, you may use the “all” parameter. *mac_phy_configuration_status* – This TLV optional data type indicates that LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port support the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disable. *link_aggregation* – This TLV optional data type indicates that LLDP agent should transmit 'Link Aggregation TLV'. This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in a aggregated link, and the aggregated port ID. The default state is disable. *maximum_frame_size* – This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is

config lldp dot3_tlvs

	disable .
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DES-3028P:4#config lldp ports all dot3_tlvs
mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs
mac_phy_configuration_status enable

Success.

DES-3028P:4#
```

config lldp forward_message

Purpose	Used to configure forwarding of lldpdu packet 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 packet will be forwarded. The default state is disable.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure the LLDP forward_lldpdu:

```
DES-3028P:4# config lldp forward_ message  enable
Command: config lldp forward_ message  enable

Success.

DES-3028P:4#
```

show lldp

Purpose	This command displays 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.

Example usage

To display the LLDP system level configuration status:

```
DES-3028P:4# show lldp
Command: show lldp

LLDP system information
    Chassis Id Subtype         : MACADDRESS
    Chassis Id                 : 00-15-E9-41-5A-A7
    System Name                : D-Link
    System Description         : Fast Ethernet Switch
    System Capabilities        : Repeater, Bridge,

LLDP Configurations
    LLDP Status                : Disable
    LLDP Forward Status        : Disable
    Message Tx Interval        : 30
    Message Tx Hold Multiplier: 4
    ReInit delay               : 2
    Tx Delay                   : 2
    Notification Interval      : 5

DES-3028P:4#
```

show lldp mgt_addr

Purpose	Used to display the lldp management address information.
Syntax	**show lldp mgt_addr {ipv4 <ipaddr>}**
Description	Displays the lldp management address information.
Parameters	*Ipv4* – IP address of IPV4.
Restrictions	None.

Example usage

To display the management address information:

```
DES-3028P:4# show lldp mgt_addr ipv4 192.168.254.10
Command: show lldp mgt_addr ipv4 192.168.254.10

Address 1:
-------------------------------------------------------
        Subtype           : IPv4
        Address           : 192.168.254.10
        IF Type           : Unknown
        OID               : 1.3.6.1.4.1.171.11.63.6
        Advertising Ports :

DES-3028P:4#
```

show lldp ports

Purpose	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>* – Specifies a range of ports to be displayed. When port list is not specified, information for all ports will be displayed.
Restrictions	None.

Example usage

To display the LLDP per port TLV option configuration:

```
DES-3028P:4# show lldp ports 1
Command: show lldp ports 1

Port ID                 : 1
----------------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Disable
Advertised TLVs Option  :
    Port Description                                      Disable
    System Name                                           Disable
    System Description                                    Disable
    System Capabilities                                   Disable
    Enabled Management Address
        (NONE.)
    Port VLAN ID                                          Disable
    Enabled VLAN Name
        (NONE.)
    Enabled protocol_identity
        (NONE.)
    MAC/PHY Configuration/Status                          Disable
    Link Aggregation                                      Disable
    Maximum Frame Size                                    Disable

DES-3028P:4#
```

show lldp local_ports

Purpose	Used to display the per-port information currently available for populating outbound LLDP advertisements.
Syntax	**show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}**
Description	This command displays the per-port information currently available for populating outbound LLDP advertisements.
Parameters	*<portlist>* – Specified a range of ports to be configured. When a port list is not specified, information for all ports will be displayed. *brief* – Display the information in brief mode. *normal* – Display the information in normal mode. This is the default display mode. *detailed* – Display the information in detailed mode.

show lldp local_ports	
Restrictions	None.

Example usage

To display outbound LLDP advertisements for individual ports in detail:

```
DES-3028P:4# show lldp local_ports 1 mode detailed
Command: show lldp local_ports 1 mode detailed

Port ID : 1
--------------------------------------------------------------------
Port Id Subtype                           : LOCAL
Port Id                                   : 1/1
Port Description                          : RMON Port  1 on Unit 1
Port PVID                                 : 1
Management Address count                  : 1
        Subtype                           : IPv4
        Address                           : 10.73.21.51
        IF Type                           : unknown
        OID                               : 1.3.6.1.4.1.171.10.64.1

VLAN Name Entries count                   : 1
    Entry 1 :
        Vlan id                           : 1
        Vlan name                         : default

Protocol Identity Entries count           : 1
    Entry 1 :
        Protocol index                    : 4
        Protocol id                       : 00 27 42 42 03 00 00 02

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

To display outbound LLDP advertisements for specific ports in normal mode:

```
DES-3028P:4# show lldp local_ports 1 mode normal
Command: show lldp local_ports 1 mode normal

Port ID : 1:
-----------------------------------------------------------
Port Id Subtype                            : LOCAL
Port Id                                    : 1/1
Port Description                           : RMON Port  1 on Unit 1
Port PVID                                  : 1
Management Address count                   : 1
VLAN Name Entries count                    : 1
Protocol Identity Entries count            : 1
MAC/PHY Configuration/Status               : (See detail)
Link Aggregation                           : (See detail)
Maximum Frame Size                         : 1522

DES-3028P:4#
```

To display outbound LLDP advertisements for specific ports in brief mode:

```
DES-3028P:4# show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief



Port ID : 1
----------------------------------------------------------
Port Id Subtype                            : LOCAL
Port Id                                    : 1/1
Port Description                           : RMON Port  1 on Unit 1

DES-3028P:4#
```

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 information learnt from the neighbor parameters. Due to the memory limitations, the switch can only receive 32 VLAN Name entries and 10 Management Address entries.
Parameters	*<portlist>* – Specified a range of ports to be configured. When a port list is not specified, information for all ports will be displayed. *brief* – Display the information in brief mode. *normal* – Display the information in normal mode. This is the default display mode. *detailed* – Display the information in detailed mode.
Restrictions	None.

Example usage

To display remote table entries in brief mode:

```
DES-3028P:4# show lldp remote_ports 1-2 mode brief
Command: show lldp remote_ports 1-2 mode brief

Port ID: 1
-----------------------------------------------------------
Remote Entities Count : 3
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-01
      Port ID Subtype               : Local
      Port ID                       : 1/3
      Port Description              : RMON Port 1 on Unit 3

Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-02
      Port ID Subtype               : Local
      Port ID                       : 1/4
      Port Description              : RMON Port 1 on Unit 4

Port ID : 2
-----------------------------------------------------------
Remote Entities Count : 3
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-03
      Port ID Subtype               : Local
      Port ID                       : 2/1
      Port Description              : RMON Port 2 on Unit 1

Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-04
      Port ID Subtype               : Local
      Port ID                       : 2/2
      Port Description              : RMON Port 2 on Unit 2

Entity 3
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-05
      Port ID Subtype               : Local
      Port ID                       : 2/3
      Port Description              : RMON Port 2 on Unit 3


DES-3028P:4#
```

To display remote table entries in normal mode:

```
DES-3028P:4# show lldp remote_ports ports 1 mode normal
Command: show lldp remote_ports ports 1 mode normal

Port ID : 1
-----------------------------------------------------------
Remote Entities Count : 2
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-01
      Port ID Subtype               : Local
      Port ID                       : 1/3
      Port Description              : RMON Port 3 on Unit 1
      System Name                   : Switch1
      System Description            : Stackable Ethernet Switch
      System Capabilities           : Repeater, Bridge
      Management Address Count      : 1
      Port VLAN ID                  : 1
      PPVID Entries Count           : 5
      VLAN Name Entries Count       : 3
      Protocol Id Entries Count     : 2
      MAC/PHY Configuration Status  : (See Detail)
      Power Via MDI                 : (See Detail)
      Link Aggregation              : (See Detail)
      Maximum Frame Size            : 1536
      Unknown TLVs Count            : 2

Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-02
      Port ID Subtype               : Local
      Port ID                       : 2/1
      Port Description              : RMON Port 1 on Unit 2
      System Name                   : Switch2
      System Description            : Stackable Ethernet Switch
      System Capabilities           : Repeater, Bridge
      Management Address Count      : 2
      Port VLAN ID                  : 1
      PPVID Entries Count           : 5
      VLAN Name Entries Count       : 3
      Protocol Id Entries Count     : 2
      MAC/PHY Configuration Status  : (See Detail)
      Power Via MDI                 : (See Detail)
      Link Aggregation              : (See Detail)
      Maximum Frame Size            : 1536

DES-3028P:4#
```

To display remote table entries in detailed mode:

```
DES-3028P:4# show lldp remote_ports 1 mode detailed
Command: show lldp remote_ports 1 mode detailed

Port ID : 1
----------------------------------------------------------------------
Remote Entities count : 1
Entity 1
    Chassis Id Subtype                    : MACADDRESS
    Chassis Id                            : 00-00-00-48-46-29
    Port Id Subtype                       : LOCAL
    Port ID                               : 1/16
    Port Description                      : RMON Port 16 on Unit 1
    System Name                           :
    System Description                    : Fast Ethernet Switch
    System Capabilities                   : Repeater, Bridge,
    Management Address count              : 1
        Entry 1 :
            Subtype                       : IPv4
            Address                       : 10.48.46.128
            IF Type                       : unknown
            OID                           : 1.3.6.1.4.1.171.11.63.9

    Port PVID                              : 1
    PPVID Entries count                    : 0
        (None.)

    VLAN Name Entries count                : 1
        Entry 1 :
            Vlan id                        : 1
            Vlan name                      : default

    Protocol ID Entries count              : 0
        (None.)

    MAC/PHY Configuration/Status           :
        Auto-negotiation support           : supported
        Auto-negotiation status            : enabled
        Auto-negotiation advertised capability : 0005(hex)
        Auto-negotiation operational MAU type  : 0010(hex)

    Power Via MDI                           :
        Port class                          : PSE
        PSE MDI power support               : supported
        PSE MDI power state                 : enabled
        PSE pairs control ability           : uncontrollable
        PSE power pair                      : 0
        power class                         : 0

    Link Aggregation                        :
        Aggregation capability              : aggregated
        Aggregation status              : not currently in aggregation
        Aggregation port ID                : 0

    Maximum Frame Size                     : 1536
    Unknown TLVs count                      : 0
        (None.)

DES-3028P:4#
```

show lldp statistics

Purpose	Used to display the system LLDP statistics information.
Syntax	**show lldp statistics**
Description	The global LLDP statistics displays an overview of neighbor detection activity on the switch.
Parameters	None.
Restrictions	None.

Example usage

To display global statistics information:

```
DES-3028P:4# show lldp statistics
Command: show lldp statistics

Last Change Time           : 6094
Number of Table Insert     : 1
Number of Table Delete     : 0
Number of Table Drop       : 0
Number of Table Ageout     : 0

DES-3028P:4#
```

show lldp statistics ports

Purpose	Used to display the ports LLDP statistics information.
Syntax	**show lldp statistics ports{<portlist>}**
Description	The per-port LLDP statistics command displays per-port LLDP statistics.
Parameters	*<portlist>* – Specified a range of ports to be configured. When a port list is not specified, information for all ports will be displayed.
Restrictions	None.

Example usage

To display statistics information of port 1:

```
DES-3028P:4# show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID: 1
-----------------------------------------------------------
      lldpStatsTxPortFramesTotal           : 27
      lldpStatsRxPortFramesDiscardedTotal  : 0
      lldpStatsRxPortFramesErrors          : 0
      lldpStatsRxPortFramesTotal           : 27
      lldpStatsRxPortTLVsDiscardedTotal    : 0
      lldpStatsRxPortTLVsUnrecognizedTotal : 0
      lldpStatsRxPortAgeoutsTotal          : 0


DES-3028P:4#
```

44

DOS PREVENTION COMMANDS

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

Command	Parameters
config dos_prevention dos_type	[{ land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024} (1) | all] {action [drop | mirror <port> { priority <value 0-7> | rx_rate [no_limit | <value 64-1024000>] }] | state [enable | disable] }
show dos_prevention	{ land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }
clear dos_prevention counters	{ land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }
enable dos_prevention trap_log	
disable dos_prevention trap_log	

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

config dos_prevention dos_type

Purpose	This command is used to discard the l3 control packets sent to CPU from specific ports.
Syntax	**config dos_prevention dos_type [{ land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024}(1) | all] {action [drop | mirror <port> { priority <value 0-7> | rx_rate [no_limit | <value 64-1024000>] }] | state [enable | disable]}**
Description	This command configures the prevention of each DoS attack, and includes state and action. The packets matching will be used by the hardware. For a specific type of attack, the content of the packet, regardless of the receipt port or destination port, will be matched against a specific pattern.
Parameters	*dos* – The type of DoS attack. Possible values are as follows: land_attack blat_attack smurf_attack tcp_null_scan tcp_xmascan tcp_synfin tcp_syn_srcport_less_1024 *state* – Used to enable or disable DoS prevention. By default, prevention for all types of DOS is enabled, except for tcp_syn_srcport_less_1024. *action* – When enabling DoS prevention, the following actions can be taken. *drop* – drop the attack packets *mirror* – mirror the packet to other port for further process.

config dos_prevention dos_type

	priority – change packet priority by the switch from 0 – 7 If the priority is not specified, the original priority will be used. *rx_rate* – controls the rate of the received DoS attack packets. If not specified, the default action is drop.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure a land attack and blat attack prevention:

```
DES-3028P:4#   config   dos_prevention   dos_type   land_attack
blat_attack state enable action drop
Command: config dos_prevention dos_type land_attack blat_attack
state enable action drop

Success.

DES-3028P:4#
```

enable dos_prevention trap_log

Purpose	Used to enable dos_prevention trap/log.
Syntax	**enable dos_prevention trap_log**
Description	This command is used to send traps and logs when a DoS attack event occurs. The event will be logged only when the action is specified as drop.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable dos_prevention trap_log:

```
DES-3028P:4# enable dos_prevention trap_log
Command: enable dos_prevention trap_log

Success.

DES-3028P:4#
```

disable dos_prevention trap_log

Purpose	Used to disable dos_prevention trap/log.
Syntax	**disable dos_prevention trap_log**
Description	This command is used to disable the dos prevention trap log.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable dos_prevention trap_log :

```
DES-3028P:4# disable dos_prevention trap_log
Command: disable dos_prevention trap_log

Success.

DES-3028P:4#
```

show dos_prevention

Purpose	Used to display DoS prevention information.
Syntax	**show dos_prevention { land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }**
Description	The show dos_prevention command displays DoS prevention information, includes the type of DoS attack, the prevention state, the corresponding action if the prevention is enabled and the counter information of the DoS packet.
Parameters	*dos* – The type of DoS attack. Possible values are as follows: • land_attack • blat_attack • smurf_attack • tcp_null_scan • tcp_xmascan • tcp_synfin • tcp_syn_srcport_less_1024
Restrictions	Only Administrator-level users can issue this command.

Example usage

To display DoS prevention information:

```
DES-3028P:4# show dos_prevention
Command: show dos_prevention
Trap/Log   : Enabled

DoS Type                        State     Action            Frame Counts
Land Attack                     Disabled  Drop              0
Blat Attack                     Enabled   Drop              123
Smurf Attack                    Enabled   Mirror            1500
TCP Null Scan                   Enabled   Drop              100000
TCP Xmascan                     Disabled  Drop              0
TCP SYNFIN                      Enabled   Mirror            1245678
TCP SYN SrcPort Less Than 1024  Enabled   Mirror            1234567890

DES-3028P:4#
```

To display DoS prevention information for Land Attack:

```
DES-3028P:4# show dos_prevention land_attack
Command: show dos_prevention land_attack

DoS Type: Land Attack
State: Enabled
Action: Mirror
      Port: 7
      Priority: 5
      Rx Rate(Kbit/sec): 1024
Frame Counts: 10000

DES-3028P:4#
```

To display DoS prevention information for Blat Attack:

```
DES-3028P:4# show dos_prevention land_attack
Command: show dos_prevention land_attack

DoS Type: Blat Attack
State: Enabled
Action: MirrorToPort
     Port: 7
     Priority: no_change
     Rx Rate(Kbit/sec): no_limit
Frame Counts: 10500

DES-3028P:4#
```

clear dos_prevention counters

Purpose	Used to clear the counters of the prevention of each DoS attack.
Syntax	**clear dos_prevention counters { land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024}**

clear dos_prevention counters	
Description	This command clears the counters of the prevention of each DoS attack.
Parameters	*dos* – The type of DoS attack. Possible values are as follows: • land_attack • blat_attack • smurf_attack • tcp_null_scan • tcp_xmascan • tcp_synfin • tcp_syn_srcport_less_1024
Restrictions	Only Administrator-level users can issue this command.

Example usage

To clear all counters of the prevention of each DoS attack:

```
DES-3028P:4# clear dos_prevention counters
Command: clear dos_prevention counters

Success.

DES-3028P:4#
```

45

IP-MAC-PORT BINDING COMMANDS

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-PORT binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC-PORT binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the DES-3028/28P/28G/52/52P series, the maximum number of IP-MAC-PORT Binding ARP mode is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

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

Command	Parameters
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ports	[<portlist> | all] state [enable {[strict | loose]} | disable]
config address_binding ip_mac ports	[<portlist> | all] allow_zeroip [enable|disable]
config address_binding ip_mac ports	[<portlist> | all] forward_dhcppkt [enable | disable]
show address_binding	[ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]
delete address_binding	[ip-mac [ipaddress <ipaddr> {mac_address <macaddr>} |all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]
enable address_binding trap_log	
disable address_binding trap_log	
show address_binding dhcp_snoop	{[max_entry {ports <portlist> | binding_entry {port <port>}]}
enable address_binding dhcp_snoop	
disable address_binding dhcp_snoop	
clear address_binding dhcp_snoop binding_entry	[<portlist> | all]

Command	Parameters
ports	
config address_binding dhcp_snoop max_entry ports	[<portlist> | all] limit [<value 1-10> | no_limit]

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

create address_binding ip_mac ipaddress

Purpose	Used to create an IP-MAC Binding entry.
Syntax	**create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}**
Description	This command will create an IP-MAC Binding entry.
Parameters	*<ipaddr>* – The IP address of the device where the IP-MAC binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC binding is made. *<portlist>* – Specifies a port or range of ports to be configured for address binding. *all* – Specifies that all ports on the switch will be configured for address binding.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DES-3028P:4#create   address_binding   ip_mac   ipaddress
10.1.1.3 mac_address 00-00-00-00-00-04
Command: create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04

Success.

DES-3028P:4#
```

config address_binding ip_mac ipaddress

Purpose	Used to configure an IP-MAC Binding entry.
Syntax	**config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}**
Description	This command will configure an IP-MAC Binding entry.
Parameters	*<ipaddr>* – The IP address of the device where the IP-MAC binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC binding is made. *<portlist>* – Specifies a port or range of ports to be configured for address binding. *all* – Specifies that all ports on the switch will be configured for address binding.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3028P:4#config   address_binding   ip_mac
ipaddress 10.1.1.3 mac_address 00-00-00-00-00-
05
Command:   config   address_binding   ip_mac
ipaddress 10.1.1.3 mac_address 00-00-00-00-00-
05

Success.

DES-3028P:4#
```

config address_binding ip_mac ports	
Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.
Syntax	**config address_binding ip_mac ports [<portlist> | all] state [enable {[strict | loose]} | disable]**
Description	This command will configure IP-MAC state to enable or disable for specified ports.
Parameters	*<portlist>* – Specifies a port or range of ports. *all* – specifies all ports on the switch. *state [enable* | *disable]* – Enables or disables the specified range of ports. *strict* – This mode provides a stricter way of control. If the user chooses *strict*, all packets will be sent to the CPU, thus all packets will not be forwarded by the hardware until the S/W learns the entries for the port. The port will check ARP packets and IP packets by IP-MAC-PORT Binding entries. The packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be dropped. The default mode is strict if not specified. *loose* – This mode provides a more loose way of control. If the user chooses *loose*, ARP packets and IP Broadcast packets will go to CPU. The packet will still be forwarded by the hardware until a specific source MAC address is blocked by the software. The port will check ARP packets and IP Broadcast packets by IP-MAC-PORT Binding entries . If the packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3028P:4#config  address_binding  ip_mac  ports  2
state enable
Command: config address_binding ip_mac ports 2 state
enable

Success.

DES-3028P:4#
```

config address_binding ip_mac ports	
Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.

config address_binding ip_mac ports

Syntax	**config address_binding ip_mac ports [<portlist> | all] allow_zeroip [enable|disable]**
Description	This command will configure IP-MAC state to enable or disable for specified ports.
Parameters	*<portlist>* – Specifies a port or range of ports. *all* – specifies all ports on the switch. *allow_zeroip [enable* | *disable]* – Enables or disables zero IP address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3028P:4#config  address_binding  ip_mac  ports  2
allow_zeroip enable
Command:  config  address_binding  ip_mac  ports  2
allow_zeroip enable

Success.

DES-3028P:4#
```

config address_binding ip_mac ports

Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.
Syntax	**config address_binding ip_mac ports** [<portlist> | all] forward_dhcppkt [enable | disable]
Description	This command will configure IP-MAC state to enable or disable forward DHCP packet for specified ports.
Parameters	*<portlist>* – Specifies a port or range of ports. *all* – specifies all ports on the switch. forward_dhcppkt [enable | disable] – Enables or disables forward DHCP packet. By default, the DHCP packet with broadcast DA will be flooded. When set to disable, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP snooping is enabled, under which case the DHCP packet which has been trapped to CPU needs to be forwarded by the software. This setting controls the forwarding behavior under this situation
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3028P:4#config  address_binding  ip_mac  ports  2
forward_dhcppkt enable
Command:  config  address_binding  ip_mac  ports  2
forward_dhcppkt enable


Success.


DES-3028P:4#
```

show address_binding

Purpose	Used to display IP-MAC Binding entries.
Syntax	**[ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]**
Description	This command will display IP-MAC Binding entries. Three different kinds of information can be viewed. • *ip_mac* – Address Binding entries can be viewed by entering the physical and IP addresses of the device. • *blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the physical address of the device. • *ports* – The number of enabled ports on a device.
Parameters	*all* – For IP_MAC binding *all* specifies all the IP-MAC binding entries; for Blocked Address Binding entries *all* specifies all the blocked VLANs and their bound physical addresses. *<ipaddr>* – The IP address of the device where the IP-MAC binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC 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 Binding on the switch:

```
DES-3028P:4#show address_binding ip_mac all
Command: show address_binding ip_mac all

IP Address      MAC Address         Mode  Ports
-------------- -----------------    ----  --------------------
10.1.1.1         00-00-00-00-00-22  arp   1-28

Total Entries: 1

DES-3028P:4#
```

delete address_binding

Purpose	Used to delete IP-MAC Binding 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 will delete IP-MAC Binding entries. Two different kinds of information can be deleted. • *IP_MAC* – Individual Address Binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to *all* will delete all the Address Binding entries. • *Blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the physical address of the device. To delete all the Blocked Address Binding entries, toggle *all.*
Parameters	<*ipaddr*> – The IP address of the device where the IP-MAC binding is made. <*macaddr*> – The MAC address of the device where the IP-MAC 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 binding *all* specifies all the IP-MAC binding entries; for Blocked Address Binding entries *all* specifies all the blocked VLANs and their bound physical addresses.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an IP-MAC Binding on the Switch:

```
DES-3028P:4#delete  address-binding  ip-mac  ipaddress  10.1.1.1  mac_address
00-00-00-00-00-06
Command: delete address-binding ip-mac ipaddress 10.1.1.1 mac_address 00-
00-00-00-00-06

Success.

DES-3028P:4#
```

enable address_binding trap_log

Purpose	Used to enable the trap log for the IP-MAC binding function.
Syntax	**enable address_binding trap_log**
Description	This command, along with the **disable address_binding trap_log** will enable and disable the sending of trap log messages for IP-MAC binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn’t match the IP-MAC binding configuration set on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable sending of IP-MAC Binding trap log messages on the Switch:

```
DES-3028P:4#enable address_binding
trap_log
Command: enable address_binding trap_log

Success.

DES-3028P:4#
```

disable address_binding trap_log

Purpose	Used to disable the trap log for the IP-MAC binding function.
Syntax	**disable address_binding trap_log**
Description	This command, along with the **enable address_binding trap_log** will enable and disable the sending of trap log messages for IP-MAC binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn’t match the IP-MAC binding configuration set on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable sending of IP-MAC Binding trap log messages on the Switch:

```
DES-3028P:4#disable       address_binding
trap_log
Command: disable address_binding trap_log

Success.

DES-3028P:4#
```

show address_binding dhcp_snoop

Purpose	To show address_binding entries created by DHCP packet.
Syntax	**show address_binding dhcp_snoop {[max_entry {ports <portlist>} | binding_entry {port <port>}]}**
Description	This command is used to show address_binding dhcp_snoop information.
Parameters	*<portlist>* – Specifies a port or range of ports. *<ports>* – Specifies ports on the device.
Restrictions	None.

Example usage:

To show address_binding dhcp_snoop:

```
DES-3028P:4# show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP_Snoop : Enabled

Success.

DES-3028P:4#
```

To show address_binding dhcp_snoop entry:

```
DES-3028P:4# show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

IP Address     MAC Address        Lease Time (secs) Port  Status
-----------   -----------------   ----------------  ----  ------
10.1.1.1      00-00-00-00-00-11       1188           1     Active

Total entries : 1

DES-3028P:4#
```

To show address_binding dhcp_snoop max_entry:

```
DES-3028P:4# show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry

Port Max entry
---- ---------
1    5
2    5
3    5
4    5
5    5
6    5
7    5
8    5
9    5
10   5
11   5
12   5
13   5
14   5
15   5
16   5
17   5
18   5
19   5
20   5
21   5
22   5
23   5
24   5
25   5
26   5

DES-3028P:4#
```

enable address_binding dhcp_snoop

Purpose	Used to enable address_binding dhcp_snoop.
Syntax	**enable address_binding dhcp_snoop**
Description	This command is used to enable the function to allow entries to be created by the DHCP packet.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To enable address_binding dhcp_snoop:

```
DES-3028P:4# enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DES-3028P:4#
```

disable address_binding dhcp_snoop

Purpose	Used to disable address_binding dhcp_snoop.
Syntax	**disable address_binding dhcp_snoop.**
Description	This command is used to disable the function which allows entries to be created by the DHCP packet.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To disable address_binding dhcp_snoop:

```
DES-3028P:4# disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DES-3028P:4#
```

clear address_binding dhcp_snoop binding_entry

Purpose	To clear the address binding entries learned for the specified ports.
Syntax	**clear address_binding dhcp_snoop binding_entry ports [<portlist> | all]**
Description	To clear the address binding entries learned for the specified ports.
Parameters	*<portlist>* – Specifies the list of ports that you would like to clear the dhcp-snoop learned entry.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To address_binding dhcp_snoop binding_entry:

```
DES-3028P:4#  clear  address_binding  dhcp_snoop  binding_entry
ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports
1-3

Success.

DES-3028P:4#
```

config address_binding dhcp_snoop max_entry

Purpose	Specifies the max number of entries which can be learned by the specified ports.
Syntax	**config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-10> | no_limit]**
Description	By default, the per port max entry is 5. This command specifies the max number of entries which can be learned by the specified ports.
Parameters	*<portlist>* – Specifies the list of ports that you would like to set the maximum dhcp-snoop learned entry. *limit* – Specifies the maximum number.
Restrictions	Only Administrator-level users can issue this command.

Example usage

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

```
DES-3028P:4# config address_binding dhcp_snoop max_entry ports
1-3 limit 10
Command: config address_binding dhcp_snoop max_entry ports 1-3
limit 10

Success.

DES-3028P:4#
```

46

LOOPBACK DETECTION COMMANDS

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

Command	Parameters
config loopdetect	{recover_timer [value 0| <value 60-1000000>] | interval <1-32767>}
config loopdetect ports	[<portlist> | all] state [enable | disable]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[<portlist> | all]

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

config loopdetect

Purpose	Used to configure loopback detection on the switch.
Syntax	**config loopdetect {recover_timer [value 0| <value 60-1000000>] | interval <1-32767>}**
Description	Used to configure loopback detection on the switch.
Parameters	*recover_timer* – The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. The valid range is *60* to *1000000*. Zero is a special value which means to disable the auto-recovery mechanism. The default value is *60*. *interval* – The time interval (in seconds) at which the remote device transmits all the CTP packets to detect the loopback event. The default value is *10*, with a valid range of *1* to *32767*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the recover time to 0, and interval to 20:

```
DES-3028P:4#config loopdetect recover_timer 0 interval 20
Command: config loopdetect recover_timer 0 interval 20

Success

DES-3028P:4#
```

config loopdetect ports

Purpose	Used to configure loopback detection on the switch.
Syntax	**config loopdetect ports [<portlist> | all] | state [enable | disable]**
Description	Used to configure loopback detection on the switch.
Parameters	*<portlist>* – Specifies a range of ports for the loopback detection *state [enable | disable]* – Allows the loopback detection to be disabled or enabled.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the loopdetect state to enable:

```
DES-3028P:4#config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success

DES-3028P:4#
```

enable loopdetect

Purpose	Used to globally enable loopback detection on the switch.
Syntax	**enable loopdetect**
Description	Used to globally enable loopback detection on the switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable loop-back detection on the switch:

```
DES-3028P:4#enable loopdetect
Command: enable loopdetect

Success

DES-3028P:4#
```

disable loopdetect

Purpose	Used to globally disable loopback detection on the switch.
Syntax	**disable loopdetect**
Description	Used to globally disable loopback detection on the switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable loop-back detection on the switch:

```
DES-3028P:4#disable loopdetect
Command: disable loopdetect

Success

DES-3028P:4#
```

show loopdetect

Purpose	Used to display the current loopback detection settings on the switch.
Syntax	**show loopdetect**
Description	Used to display the current loopback detection settings on the switch
Parameters	None.
Restrictions	None.

Example usage:

To show loopdetect:

```
DES-3028P:4#show loopdetect
Command: show loopdetect

 Loopdetect Global Settings
 ---------------------------
 Loopdetect Status          : Enabled
 Loopdetect Interval        : 20
 Recover Time               : 60

DES-3028P:4#
```

show loopdetect ports

Purpose	Used to display the current per-port loopback detection settings on the switch.
Syntax	**show loopdetect ports [<portlist> | all]**
Description	Used to display the current per-port loopback detection settings on the switch
Parameters	*<portlist>* – Specifies a range of ports for the loopback detection *all* – Specifies all ports for the loopback detection.
Restrictions	None.

Example usage:

To show loopdetect ports:

```
DES-3028P:4#show loopdetect ports 1-3
Command: show loopdetect ports 1-3

Port   Loopdetect State    Loop Status
------ ----------------- ----------
1      Enabled             Normal
2      Enabled             Normal
3      Enabled             Normal

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

47

TECHNICAL SUPPORT COMMANDS

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

Command	Parameters
show tech_support	
upload tech_support_to_TFTP	<ipaddr> <path_filename 64>

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

show tech_support	
Purpose	Used to show the information for technical support.
Syntax	**show tech_support**
Description	This command is especially used by the technical support personnel to dump the device’s overall operation information. The information is project dependent and includes the following information. Basic System information system log Running configuration Layer 1 information Layer 2 information Application OS status
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To display technical support information on the Switch:

```
DES-3028P:4# show tech_support
Command: show tech_support

[Device Information 3049620ms]
Device Type        : DES-3028G Fast Ethernet Switch
MAC Address        : 00-21-91-98-60-77
IP Address         : 10.73.21.11 (Manual)
VLAN Name          : default
Subnet Mask        : 255.0.0.0
Default Gateway    : 0.0.0.0
Boot PROM Version  : Build 1.00.B06
Firmware Version   : Build 2.00.B23
Hardware Version   : 1A1G
Serial number      : P4IG188000007
Spanning Tree      : Disabled
GVRP               : Disabled
IGMP Snooping      : Disabled
802.1x             : Disabled
TELNET             : Enabled(TCP  23)
WEB                : Enabled(TCP  80)
RMON               : Disabled
SSH                : Disabled
SSL                : Disabled
Syslog Global State: Disabled
Dual Image         : Supported
Password Encryption Status : Disabled.

[CUP Utilization 3049620ms]
CPU Utilization :
--------------------------------------------------------------------------
Five Seconds -   1 %         One Minute -   1 %         Five Minutes -   2 %

[Connection Session Status 3049620ms]
ID   Login Time           Live Time        From         Level   Name
--  -------------------  ------------  ---------------  -----  -----------
8   0/00/00  00:46:34    0:4:14.240    Serial Port      4      Anonymous

Total Entries: 1
[Unicast FDB Table 3049620ms]
VID  MAC Address       Port Type
---- ----------------- ---- ---------------
1    00-00-00-48-46-29  3   Dynamic
1    00-00-5E-00-01-5F  3   Dynamic
1    00-00-81-00-00-01  3   Dynamic
1    00-00-81-9A-F2-F4  3   Dynamic
1    00-01-01-01-22-22  3   Dynamic
1    00-01-06-30-00-00  3   Dynamic
1    00-01-11-22-33-02  3   Dynamic
1    00-02-A5-FD-66-97  3   Dynamic
```

```
1    00-03-09-18-10-01  3   Dynamic
1    00-04-00-00-00-00  3   Dynamic
1    00-05-5D-04-D6-A4  3   Dynamic

Total Entries  : 264

DES-3028P:4#
```

upload tech_support_to_TFTP

Purpose	Used to upload the information of technical support.
Syntax	upload tech_support_to_TFTP <ipaddr> <path_filename>
Description	The upload tech_support_to_TFTP command is used to upload the technical support information.
Parameters	*<ipaddr>* – Specifies the ipaddress of TFTP server. *<path_filename>* – Specifies the file path to store the information of technique's support in TFTP server.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To upload the technical support information:

```
DES-3028P:4# upload tech_support_to_tftp 10.55.47.1 tech_report_20080423.txt
Command: upload tech_support_to_tftp 10.55.47.1 tech_report_20080423.txt

Connecting to server................... Done.
Upload technique support information... Done.

Success.
```

48

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
?	
dir	
config command_history	<value 1-40>
show command_history	

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

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	**? {<command>}**
Description	This command 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-3028P:4#?
..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear dos_prevention counters
clear fdb
clear igmp_snooping data_driven_group
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display the parameters for a specific command:

```
DES-3028P:4# config stp
Command:? config stp

Command: config stp
Usage: {maxage <value 6-40> | maxhops <value1-20> | hellotime
<value 1-10> | forwarddelay <value 4-30> | txholdcount <value
1-10> | fbpdu [enable | disable] | lbd [enable | disable] |
lbd_recover_timer [0 | <value 60-1000000>]}
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-3028P:4#
```

dir	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	**dir**
Description	This command will display all of the commands available through the Command Line Interface (CLI).

dir

Parameters	None.
Restrictions	None.

Example usage:

To display all commands:

```
DES-3028P:4#dir
..
?
clear
clear arptable
clear counters
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config admin local_enable
config arp_aging time
config arpentry
config authen application
CTRL+C  ESC  q  Quit  SPACE  n  Next  Page  ENTER  Next
Entry a All
```

config command_history

Purpose	Used to configure the command history.
Syntax	**config command_history <value 1-40>**
Description	This command is used to configure the command history.
Parameters	<*value 1-40*> – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	None.

Example usage

To configure the command history:

```
DES-3028P:4#config command_history 20
Command: config command_history 20

Success.
```

```
DES-3028P:4#
```

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-3028P:4#show command_history
Command: show command_history

?
? show
show vlan
show command history

DES-3028P:4#
```

Appendix A

TECHNICAL SPECIFICATIONS

General	
Protocols	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP “Mini GBIC”) IEEE 802.1D/s/w Spanning Tree IEEE 802.1Q VLAN IEEE 802.1p Priority Queues IEEE 802.1X Port Based Network Access Control IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 NWay auto-negotiation IEEE802.3af standard (only for POE)
Fiber-Optic	SFP (Mini GBIC) Support: DEM-310GT (1000BASE-LX) DEM-311GT (1000BASE-SX) DEM-314GT (1000BASE-LH) DEM-315GT (1000BASE-ZX) DEM-210 (Single Mode 100BASE-FX) DEM-211 (Multi Mode 100BASE-FX) WDM Transceivers Supported: DEM-330T (TX-1550/RX-1310nm), up to 10km, Single-Mode DEM-330R (TX-1310/RX-1550nm), up to 10km, Single-Mode DEM-331T (TX-1550/RX-1310nm), up to 40km, Single-Mode DEM-331R (TX-1310/RX-1550nm), up to 40km, Single-Mode
Standards	CSMA/CD
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
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)
Number of Ports	DES-3028/DES-3028P: 24 x 10/100Base-T Ports 2 x 1000Base-T/SFP Combo Ports 2 x 1000Base-T ports DES-3028G: 24 x 10/100Base-T Ports 4 x 1000Base-T/SFP Combo Ports DES-3052/DES-3052P: 48 x 10/100Base-T Ports 2 x 1000Base-T/SFP Combo Ports 2 x 1000Base-T ports

Physical and Environmental	
Internal Power Supply	Input: DES-3028/DES-3052/DES-3028G - 100~240V, AC/0.5A, 50~60Hz DES-3052P - 100~240V, AC/5A, 50~60Hz DES-3028P - 100~240V, AC/2.9A, 50~60Hz Output: DES-3028/DES-3052/DES-3028G: 12V, 3.3A (Max) DES-3028P: 12V, 3.3A/50V, 3.7A (Max) DES-3052P: 12V,10.5A/50V,7.5A (Max)
Power Consumption	DES-3028 – 18.8W DES-3052 – 25.5W DES-3028G –15.6W DES-3028P – 217W DES-3052P – 395W
DC Fans	DES-3028/DES-3052/DES-3028G – None DES-3028P – one 8.5cm fan and one 17cm fan DES-3052P – one 5cm fan, one 8.3cm fan, and one 17cm fan
Operating Temperature	0 - 40°C
Storage Temperature	-40 - 70°C
Humidity	5 - 95% non-condensing
Dimensions	DES-3028/DES-3028G: 441(W) x 207(D) x 44(H) mm DES-3028P/3052/3052P: 441(W) x 309(D) x 44(H) mm
Weight	DES-3028 – 2.36kg (5.20lbs) DES-3028G – 2.42kg (5.33lbs) DES-3028P – 4.5kg (9.9lbs) DES-3052 – 3.85kg (8.48lbs) DES-3052P – 5.70kg (12.56lbs)
EMI	CE Class A, FCC Class A, C-Tick, VCCI
Safety	CB Report, UL

Performance	
Transmission Method	Store-and-forward
Packet Buffer	512 KB per device
Packet Filtering/ Forwarding Rate	14,881 pps (10M port) 148.810 pps (100M port) 1,488,100 pps (1Gbps port)
MAC Address Learning	Automatic update. Supports 8K MAC address
Priority Queues	4 Priority Queues per port.

Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.

<table>
<tr><th colspan="2">PoE Features</th></tr>
<tr><td>PoE Capable Ports</td><td>DES-3028P:Random 12 ports
DES-3052P:Random 24 ports
Max 15.4W per port</td></tr>
<tr><td>Power feeding for PoE</td><td>DES-3028P:
Per port →15.4W (Default),
Output capacity for DES-3028P→185W
DES-3052P:
Per port →15.4W (Default),
Output capacity for DES-3052P→370W</td></tr>
<tr><td>PoE Specification</td><td>Supplies power to PD device up to 15.4W per port, meeting IEEE802.3af standards and more sufficiently is able to provide power to PD devices
Auto discovery feature, automatically recognize the connection of PD device and immediately sends power to it
Auto disable port if the port current is over 350mA while other ports remain active
Active circuit protection, automatically disables the port if there is a short while other ports remain active
PD should be able to receive the power following the classification below
<table>
<tr><th>Class</th><th>Usage</th><th>Max power used by PD</th></tr>
<tr><td>0</td><td>Default</td><td>0.44 to 12.95W</td></tr>
<tr><td>1</td><td>Optional</td><td>0.44 to 3.84W</td></tr>
<tr><td>2</td><td>Optional</td><td>3.84 to 6.49W</td></tr>
<tr><td>3</td><td>Optional</td><td>6.49 to 12.95W</td></tr>
<tr><td>4</td><td>Not allowed</td><td>Reserved</td></tr>
</table>
PSE should be provide the power following the classification below
<table>
<tr><th>Class</th><th>Usage</th><th>Max power used by PD</th></tr>
<tr><td>0</td><td>Default</td><td>15.4W</td></tr>
<tr><td>1</td><td>Optional</td><td>4.0W</td></tr>
<tr><td>2</td><td>Optional</td><td>7.0W</td></tr>
<tr><td>3</td><td>Optional</td><td>15.4W</td></tr>
<tr><td>4</td><td>Reserved</td><td>15.4W</td></tr>
</table>
DES-3028P/DES-3052P should follow the standard PSE pin-out standard of Alternative A which is sending out power over number 1,2,3,6 pins of 8 wires of CAT5 UTP cable
DES-3028P/DES-3052P works with all D-Link 802.3af capable devices
9. DES-3028P/DES-3052P works with all non-802.3af capable D-Link AP, IP Cam and IP phone via DWL-P50</td></tr>
</table>

LED Indicators

Location	LED Indicative	Color	Status	Description
Per Device	**Power**	Green	Solid Light	Power On
			Light off	Power Off
	Console	Green	Solid Light	Console on
			Blinking	POST is in progress/ POST is failure.
			Light off	Console off
“Mode Select Button” (only for DES-3028P/DES-3052P)	**Link/Act/ Speed**	Green	Solid Light	Link/Act/Speed Mode
	PoE	Green	Solid Light	PoE Mode
LED Per 10/100 Mbps Port	**Link/Act/Speed**	Green/Amber	Solid Green	When there is a secure 100Mbps Fast Ethernet connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a Fast Ethernet connected port.
			Solid Amber	When there is a secure 10Mbps Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at an Ethernet connected port.
			Light off	No link
	PoE (only for DES-3028P/DES-3052P)	Green	Solid Green	Powered device is connected.
			Blinking	Port has detected a error condition
			Light off	Powered Device may receive power from an AC power source or no 802.3af PD is found.
LED Per GE Port	**Link/Act/Speed mode for 1000BASE-T ports**	Green/Amber	Solid Green	When there is a secure 1000Mbps connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity--Act) of data occurring at a 1000Mbps connected port.
			Solid Amber	When there is a secure 10/100Mbps Fast Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at a Fast Ethernet connected port.
			Light off	No link
	Link/Act/Speed mode for SFP ports	Green/Amber	Solid Green	When there is a secure 1000Mbps connection (or link) at the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity--Act) of data occurring at a 1000Mbps connected port.
			Solid Amber	When there is a secure 100Mbps connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at the ports.

			Light off	No link

Power

Feature	Detailed Description
Internal Power Supply	AC Input: 100 - 240 VAC, 50-60 Hz

Performance

Feature	Detailed Description
Wire speed on all FE/GE ports	Full-wire speed (full-duplex) operation on all FE/GE ports
Forwarding Mode	Store and Forward
Switching Capacity	12.8Gbps for DES-3028/DES-3028P/DES-3028G 17.6Gbps for DES-3052/DES-3052P
64 Byte system packet forwarding rate	9.5 million packets per second for DES-3028/DES-3028P/DES-3028G 13.1 million packets per second for DES-3052/DES-3052P
Priority Queues	4 Priority Queues per port
MAC Address Table	Supports 8K MAC address
Packet Buffer Memory	512K Bytes

Port Functions

Feature	Detailed Description
Console Port	DCE RS-232 DB-9 for out-of-band configuration of the software features
24 x 10/100BaseT ports 48 x 10/100BaseT ports (Power over LAN support)	Compliant to following standards, IEEE 802.3 compliance IEEE 802.3u compliance Support Half/Full-Duplex operations All ports support Auto MDI-X/MDI-II cross over IEEE 802.3x Flow Control support for Full-Duplex mode, Back Pressure when Half-Duplex mode, and Head-of-line blocking prevention. Compliant IEEE802.3af standard(only for PoE)
Combo ports in the front panel	combo 1000BASE-T/SFP ports 1000BASE-T ports compliant to following standards: IEEE 802.3 compliance IEEE 802.3u compliance IEEE 802.3ab compliance Support Full-Duplex operations IEEE 802.3x Flow Control support for Full-Duplex mode, back pressure when Half-Duplex mode, and Head-of-line blocking prevention SFP Transceivers Supported: DEM-310GT (1000BASE-LX) DEM-311GT (1000BASE-SX)

	DEM-314GT (1000BASE-LH) DEM-315GT (1000BASE-ZX) DEM-210 (Single Mode 100BASE-FX) 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-1550nm), up to 10km,Single-Mode 3.DEM-331T (TX-1550/RX-1310nm), up to 40km, Single-Mode 4.DEM-331R (TX-1310/RX-1550nm), up to 40km, Single-Mode Compliant to following standards: IEEE 802.3z compliance IEEE 802.3u compliance
1000BASE-T ports in the front panel	1000BASE-T ports compliant to following standards: 1. IEEE 802.3 compliance 2. IEEE 802.3u compliance 3. IEEE 802.3ab compliance 4. Support Full-Duplex operations 5. IEEE 802.3x Flow Control support for Full-Duplex mode, back pressure when Half-Duplex mode, and Head-of-line blocking prevention

Pin Assignment for Data/Power Pairs: (alternative A MDI-X)

PIN#	Signal	Descriptions
1	Receive+ & Power-	0V
2	Receive- & Power-	0V
3	Transmit+ & Power+	+48V
4		
5		
6	Transmit- & Power+	+48V
7		
8		

Appendix B

ARP 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 so hackers 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 countermeasure devised by D-Link to put an end to ARP spoofing attacks.

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.

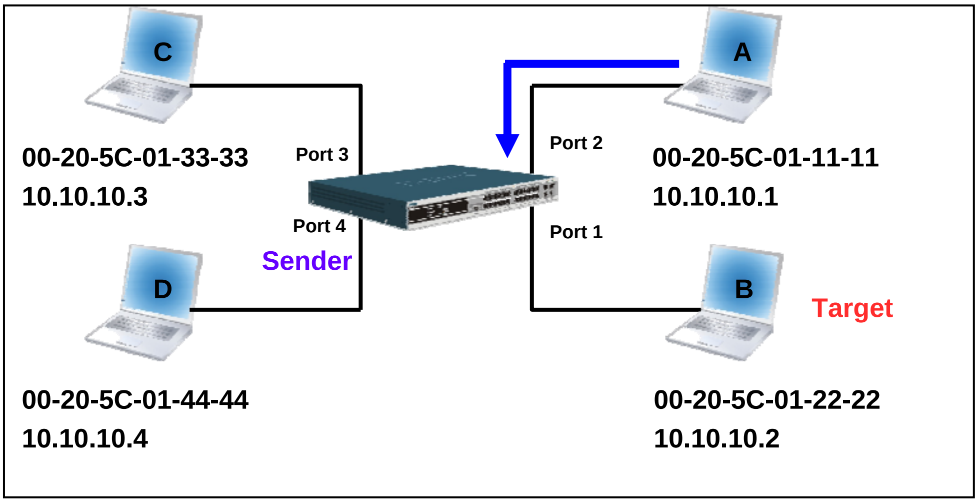


Figure – 1

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***	***10.10.10.1***	***00-00-00-00-00-00***	***10.10.10.2***

Table – 1 (ARP Payload)

The ARP request will be encapsulated into the 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 the ARP request is sent via a broadcast method, the "Destination address" is in the format of 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 and enter them in its Forwarding Table.

Forwarding Table

Port1 00-20-5C-01-11-11

In addition, when the switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure – 2).

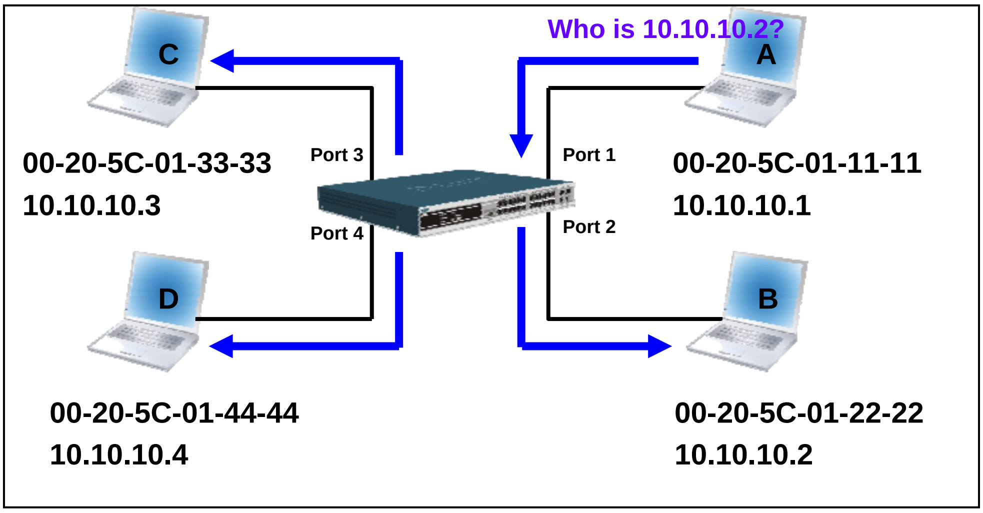


Figure – 2

When the switch floods the frame of the ARP request to the network, all PCs will receive and examine the frame but only PC B will reply to the query because the destination IP matches (see Figure – 3).

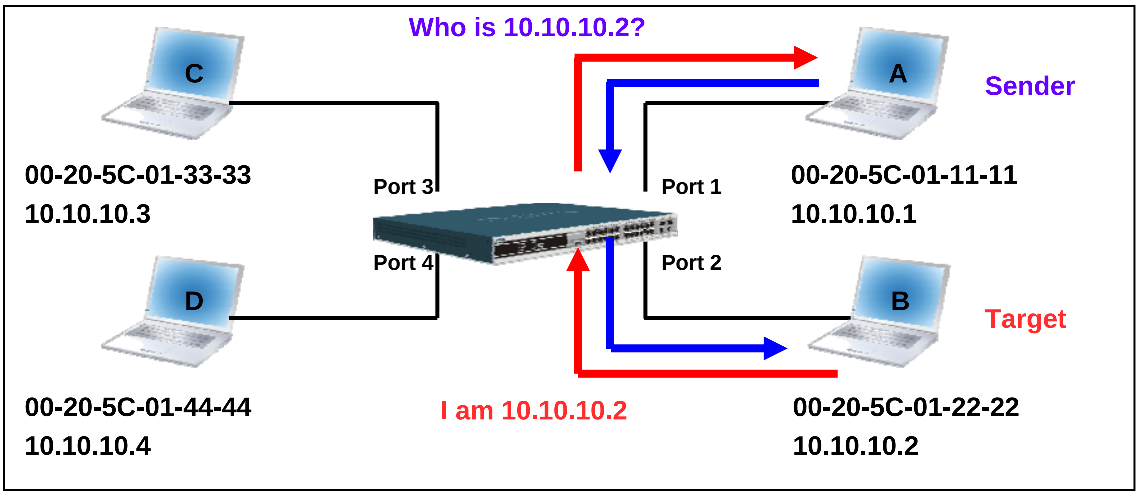


Figure – 3

When PC B replies to an ARP request, its MAC address will be written into the "Target H/W Address" table 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 the form of a 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	***00-20-5C-01-11-11***	***10.10.10.1***	***00-20-5C-01-22-22***	***10.10.10.2***

Table – 3 (ARP Payload)

When PC B replies to the query, “Destination Address” in the Ethernet frame it will change 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
00-20-5C-01-11-11	***00-20-5C-01-22-22***			

Table – 4 (Ethernet frame format)

The switch will also examine the “Source Address” of the Ethernet frame and if it finds 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 addresses 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 attacks are caused by Gratuitous ARPs that occur when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

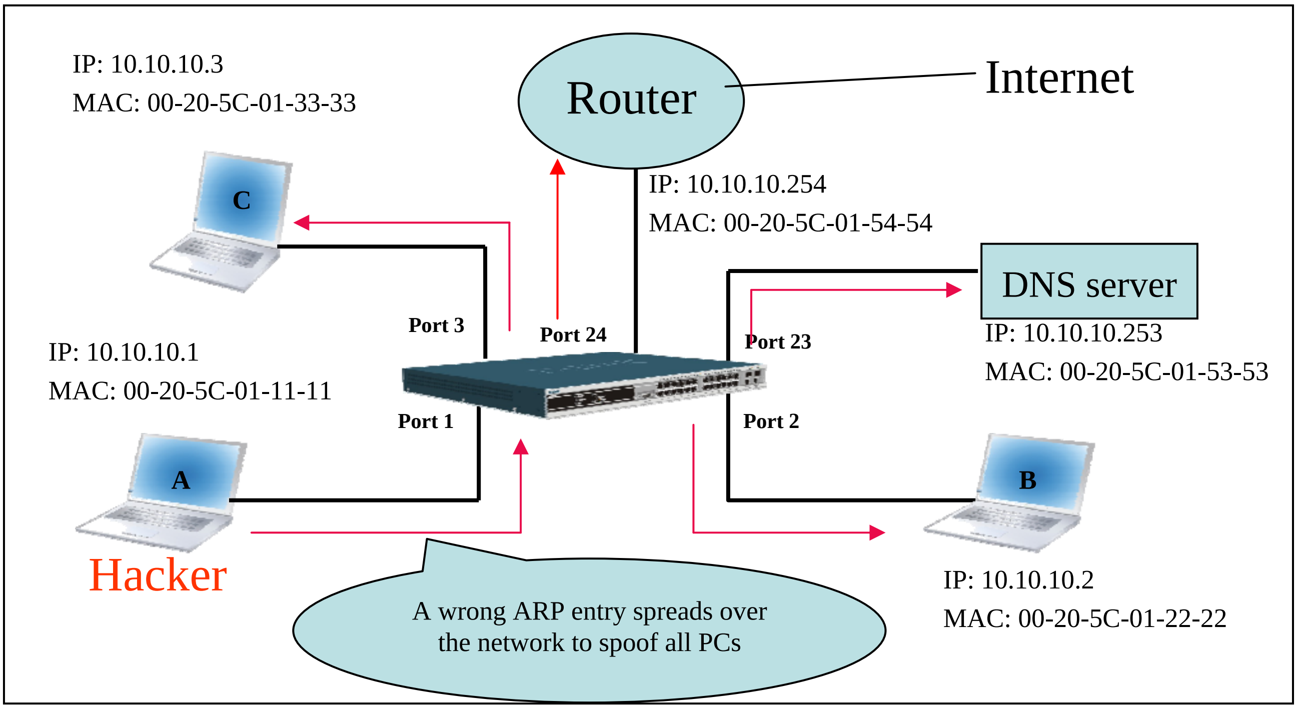


Figure – 4

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address itself. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address. 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**	***00-20-5C-01-11-11***	***10.10.10.254***	***00-20-5C-01-11-11***	***10.10.10.254***

Table – 5

A common DoS attack today can be done by associating a nonexistent or any specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast ONE Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets sent through 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 fools the victims PC to make it believe it is a router and fools the router to make it believe it is the victim. As can be seen in Figure-5 all traffic will be then sniffed by the hacker without the users knowledge.

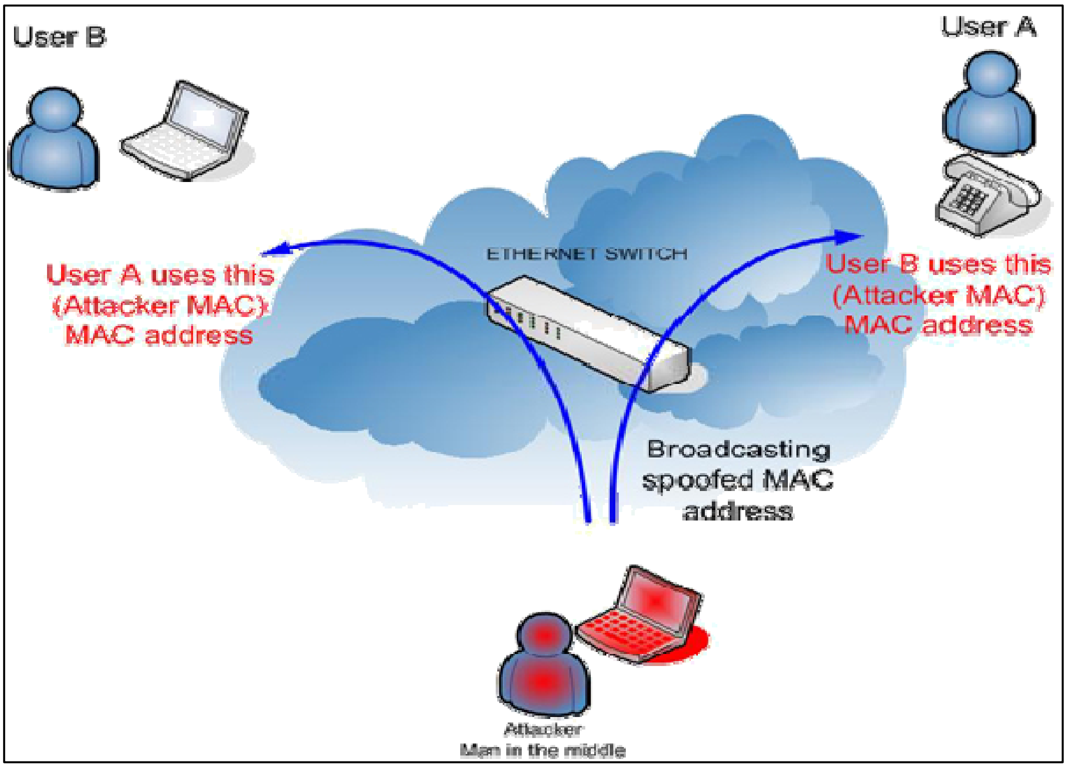
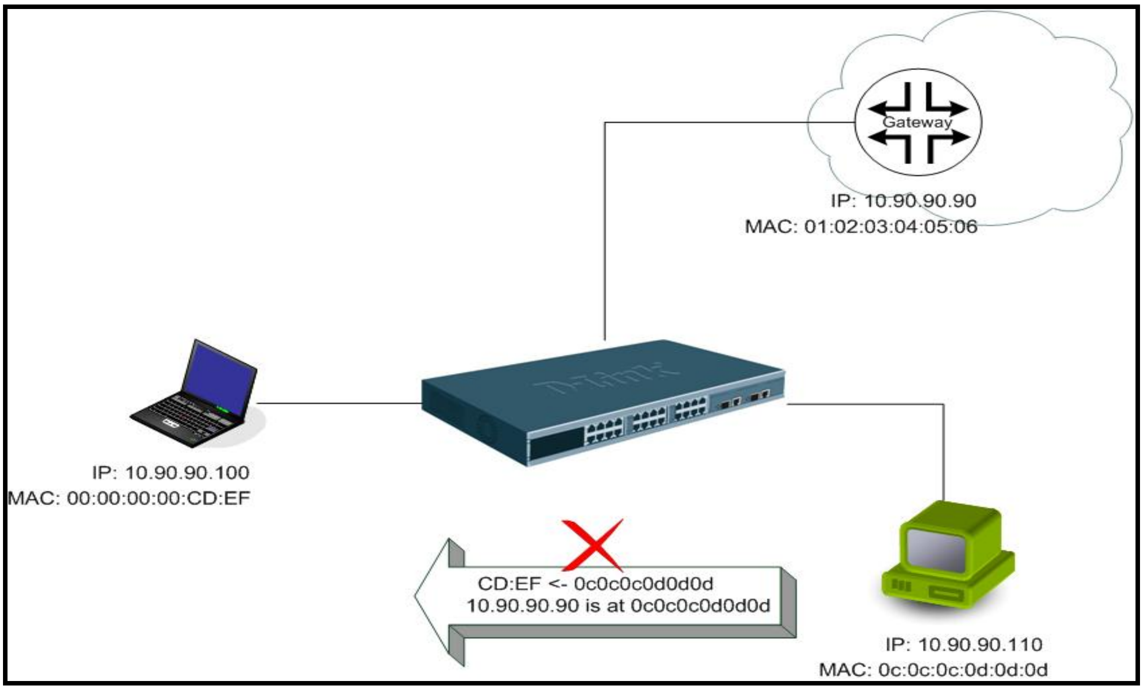

User B
User A
ETHERNET SWITCH
User A uses this (Attacker MAC) MAC address
User B uses this (Attacker MAC) MAC address
Broadcasting spoofed MAC address
Attacker
Man in the middle

Figure – 5

Prevent ARP spoofing via packet content ACL

Concerning the common DoS attack today caused by the ARP spoofing, D-Link managed switches can effectively mitigate it via its unique Packet Content ACL.

The reason for this is that basic ACLs can only filter ARP packets based on packet type, VLAN ID, Source and Destination MAC information, therefore there is a need for further inspections of ARP packets. To prevent ARP spoofing attacks, we will demonstrate here using the Packet Content ACL on the DES-3028 block the invalid ARP packets which contain faked gateway's MAC and IP binding.



Example Topology

Configuration:

The design of the Packet Content ACL on the DES-3028/28P/28G/52/52P series can inspect any specified content in the first 20 bytes of an ARP packet (up to 80 bytes in total at one time). It utilizes offsets to match individual fields in the Ethernet Frame. An offset contains 16 bytes and the switch supports 5 offsets with each offset being divided into a four 4-byte values in a HEX format. The offset ranges from 0-76. (Refer to the configuration example below for details)

In addition, the configuration logics are:

1. Only if the ARP matches the Source MAC addresses in Ethernet, Sender's MAC address and Senders IP address in the ARP protocol can it 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.

When calculating packet offset on DES-3028/28P/28G/52/52P series, remember that even though a port is an untagged port, the packet will add additional **4 bytes** of 802.1Q header (TCI) for switching internal process, shown in Figure – 6.

All packets will add an additional 4 bytes to assign PVID for the switching internal process.

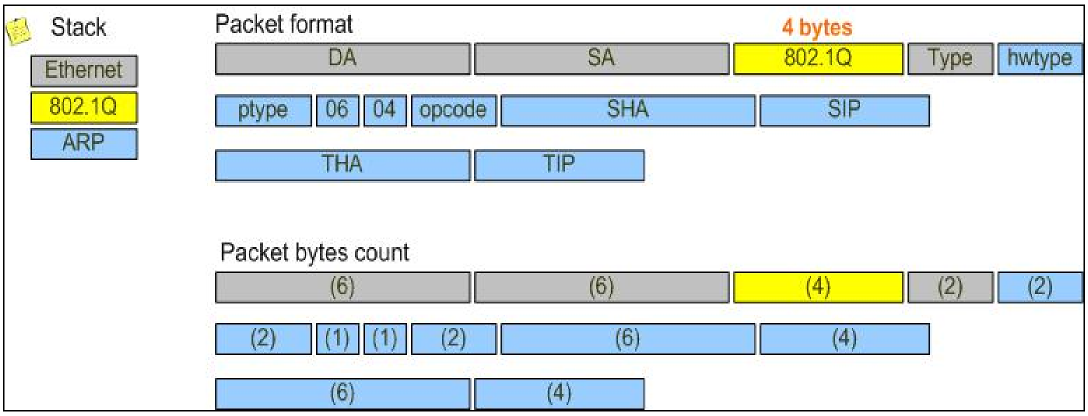
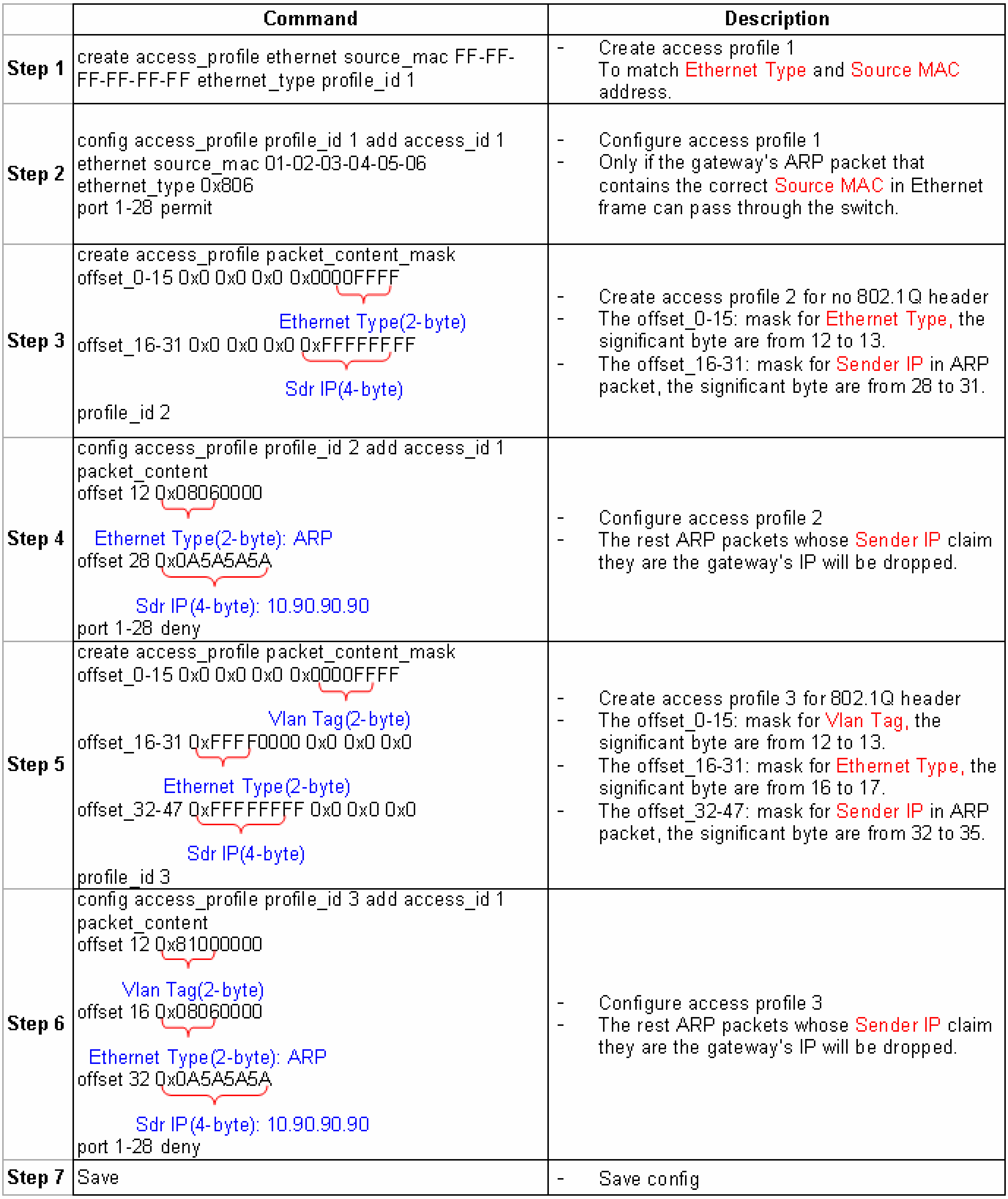

Stack
Ethernet
802.1Q
ARP
Packet format
4 bytes
DA
SA
802.1Q
Type
hwtype
ptype
06
04
opcode
SHA
SIP
THA
TIP
Packet bytes count
(6)
(6)
(4)
(2)
(2)
(2)
(1)
(1)
(2)
(6)
(4)
(6)
(4)

Figure – 6



	Command	Description
Step 1	create access_profile ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type profile_id 1	- Create access profile 1 To match Ethernet Type and Source MAC address.
Step 2	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-28 permit	- Configure access profile 1 - Only if the gateway's ARP packet that contains the correct Source MAC in Ethernet frame can pass through the switch.
Step 3	create access_profile packet_content_mask offset_0-15 0x0 0x0 0x0 0x0000FFFF Ethernet Type(2-byte) offset_16-31 0x0 0x0 0x0 0xFFFFFFFF Sdr IP(4-byte) profile_id 2	- Create access profile 2 for no 802.1Q header - The offset_0-15: mask for Ethernet Type, the significant byte are from 12 to 13. - The offset_16-31: mask for Sender IP in ARP packet, the significant byte are from 28 to 31.
Step 4	config access_profile profile_id 2 add access_id 1 packet_content offset 12 0x08060000 Ethernet Type(2-byte): ARP offset 28 0x0A5A5A5A Sdr IP(4-byte): 10.90.90.90 port 1-28 deny	- Configure access profile 2 - The rest ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step 5	create access_profile packet_content_mask offset_0-15 0x0 0x0 0x0 0x0000FFFF Vlan Tag(2-byte) offset_16-31 0xFFFF0000 0x0 0x0 0x0 Ethernet Type(2-byte) offset_32-47 0xFFFFFFFF 0x0 0x0 0x0 Sdr IP(4-byte) profile_id 3	- Create access profile 3 for 802.1Q header - The offset_0-15: mask for Vlan Tag, the significant byte are from 12 to 13. - The offset_16-31: mask for Ethernet Type, the significant byte are from 16 to 17. - The offset_32-47: mask for Sender IP in ARP packet, the significant byte are from 32 to 35.
Step 6	config access_profile profile_id 3 add access_id 1 packet_content offset 12 0x81000000 Vlan Tag(2-byte) offset 16 0x08060000 Ethernet Type(2-byte): ARP offset 32 0x0A5A5A5A Sdr IP(4-byte): 10.90.90.90 port 1-28 deny	- Configure access profile 3 - The rest ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step 7	Save	- Save config

Appendix C

PASSWORD RECOVERY PROCEEDURE

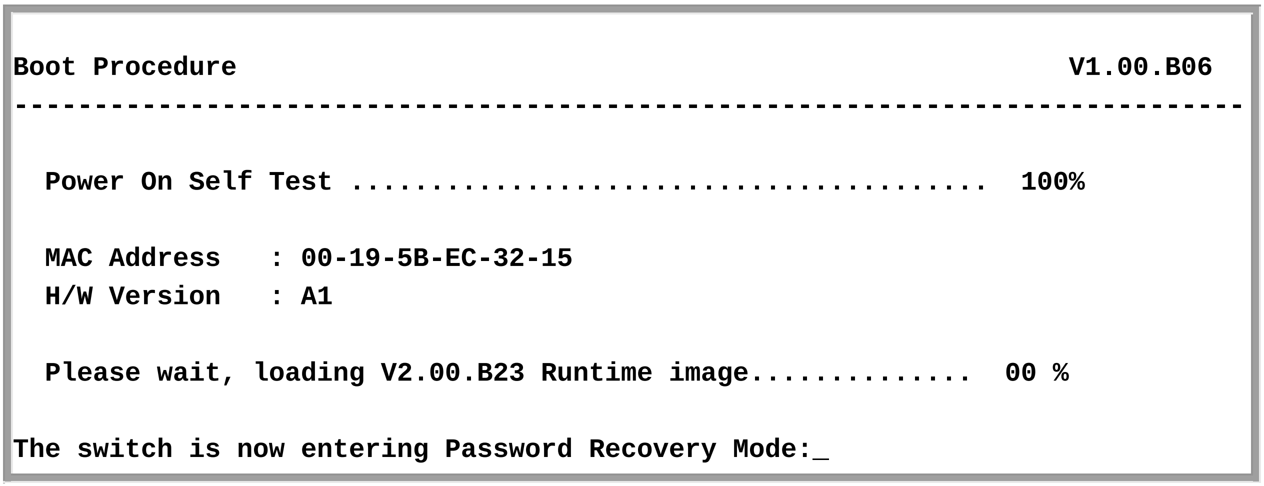
This document describes the procedure for resetting passwords on D-Link Switches.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This document will explain how the Password Recovery feature can help network administrators reach this goal.

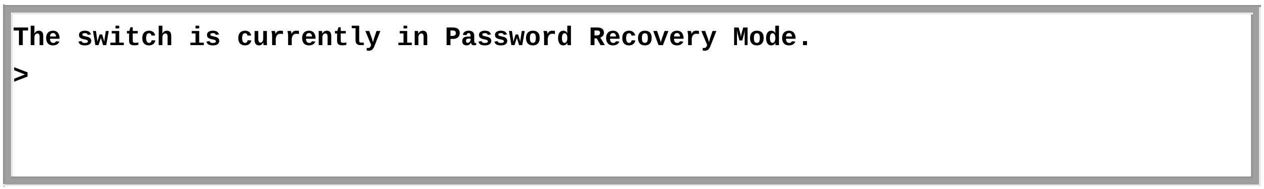
The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the switch. After the runtime image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode”. Once the Switch enters the “Password Recovery Mode”, all ports on the Switch will be disabled.



```
Boot Procedure                                                     V1.00.B06
-----------------------------------------------------------------------------

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

  MAC Address   : 00-19-5B-EC-32-15
  H/W Version   : A1

  Please wait, loading V2.00.B23 Runtime image.............  00 %

The switch is now entering Password Recovery Mode:_
```



```
The switch is currently in Password Recovery Mode.
>
```

3. In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
reset config	The reset config command resets the whole configuration 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	The reset password command resets the password of the specified

Command	**Parameters**
{<username>}	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.