D-Link®

DES-3010F/DES-3010FL/DES-3010G/DES-3018/DES-3026

Managed 8/16/24-port 10/100Mbps N-Way Fast Ethernet Switch

Command Line Interface Reference Manual

Fourth Edition (May 2007)

651ES3026045G

Printed In Taiwan

RECYCLABLE

Table of Contents

1

INTRODUCTION

This document is a reference guide for all DES-3010F/DES-3010FL/DES-3010G/DES-3018/DES-3026 switches. Throughout this manual, the DES-3026 Switch will be the Switch referred to for all examples and configuration information. All DES-3010F/DES-3010FL /DES-3010G/DES-3018/DES-3026 switches contain the same information and posses the same configuration capabilities. The difference in switches reside in the port type and the port count only.

The DES-3026 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 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 is then connected to the Switch's serial port via an RS-232 DB-9 cable.

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

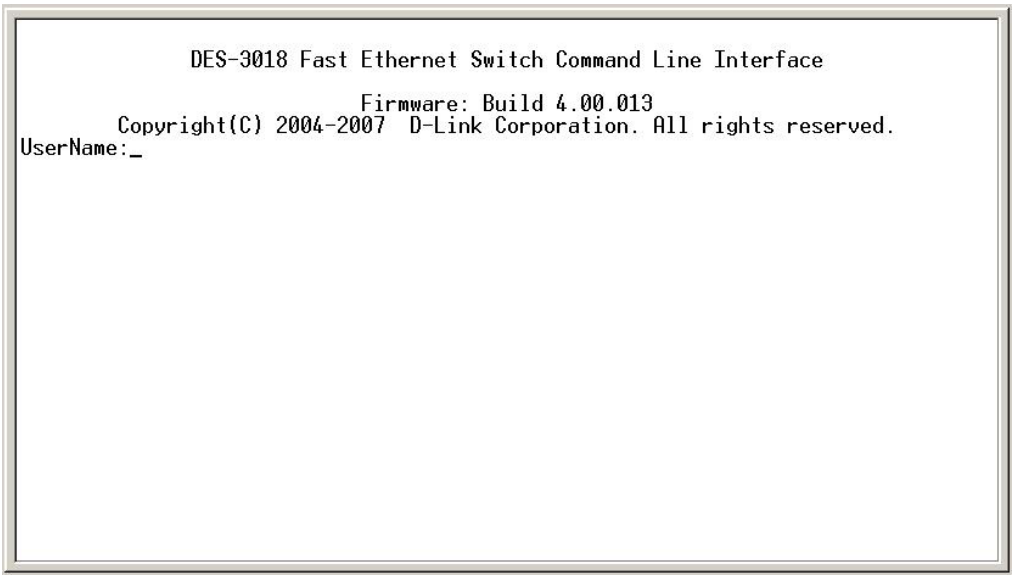

Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-3026:4#**. 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. The default Switch IP address can be changed 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.

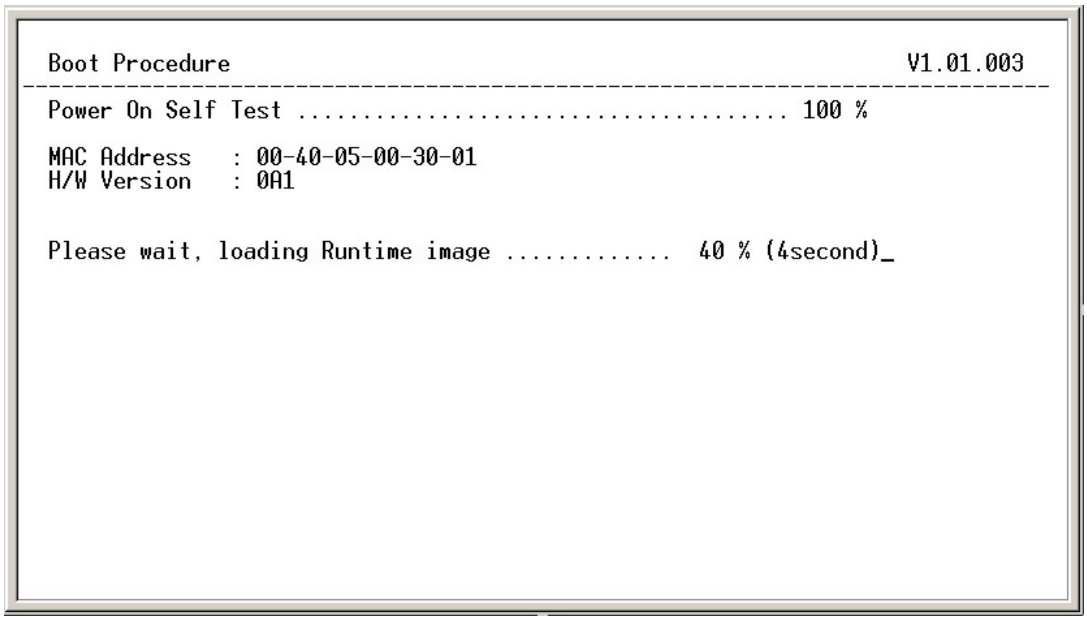

Figure 1-2. Boot Screen

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

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

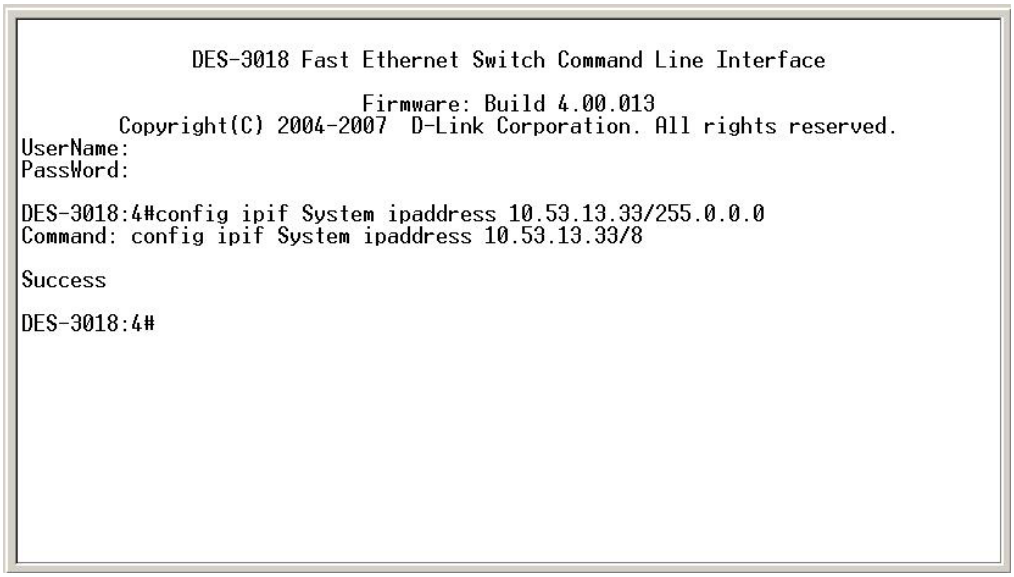

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.53.13.33 with a subnet mask of 255.0.0.0 (8 in CIDR from). The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet 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-3026 supports a console management interface that allows the user to connect to the Switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the Switch to use an SNMP-based network management software over the network.

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

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

Connecting to the Switch

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

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

You can also access the same functions over a Telnet interface. Once you have set an IP address for your Switch, you 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 you have logged in, the console looks like this:

```
            DES-3018 Fast Ethernet Switch Command Line Interface

                          Firmware: Build 4.00.013
       Copyright(C) 2004-2007  D-Link Corporation. All rights reserved.
UserName:
PassWord:

DES-3018:4#
```

Figure 2-1. Console Screen after login

Commands are entered at the command prompt, **DES-3026:4#**.

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.

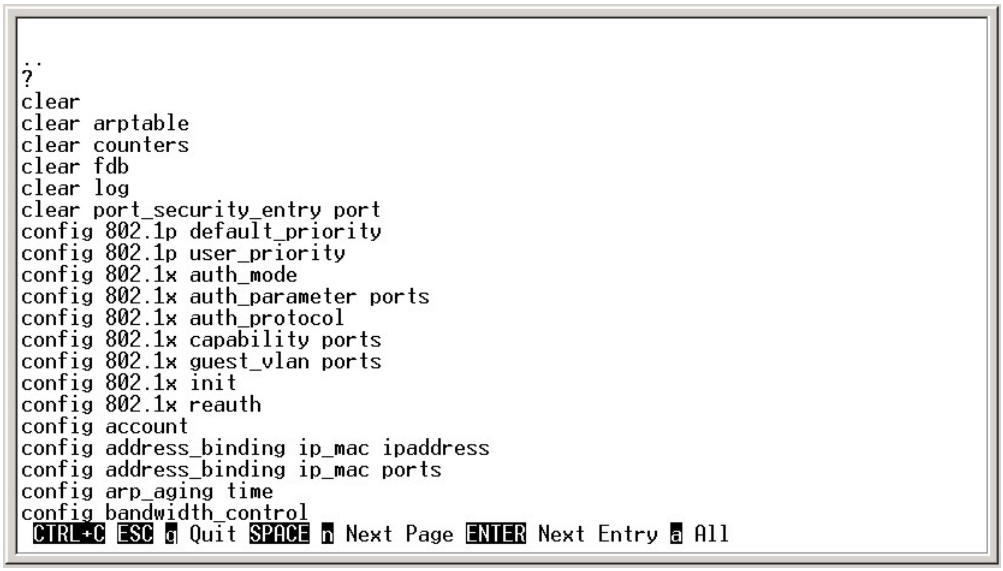

Figure 2-2. The ? Command

The **dir** command has the same function as the **?** command.

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

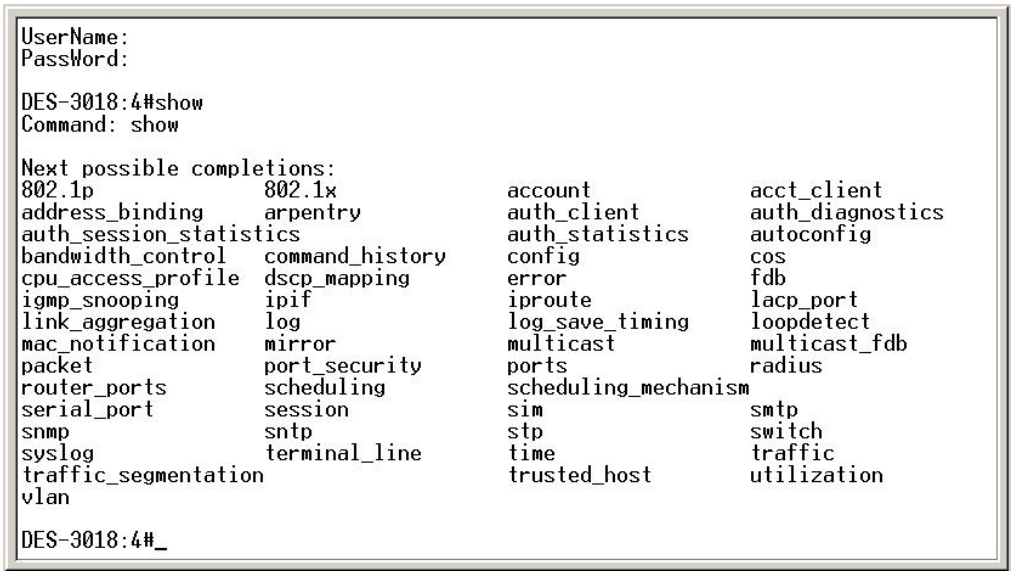

Figure 2-3. Example Command Parameter Help

In this case, the command **show** was entered without a parameter. The CLI will then prompt you to enter the **next possible completions** 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, you can see all of the next possible sub-commands, in sequential order, by repeatedly pressing the **Tab** key.

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

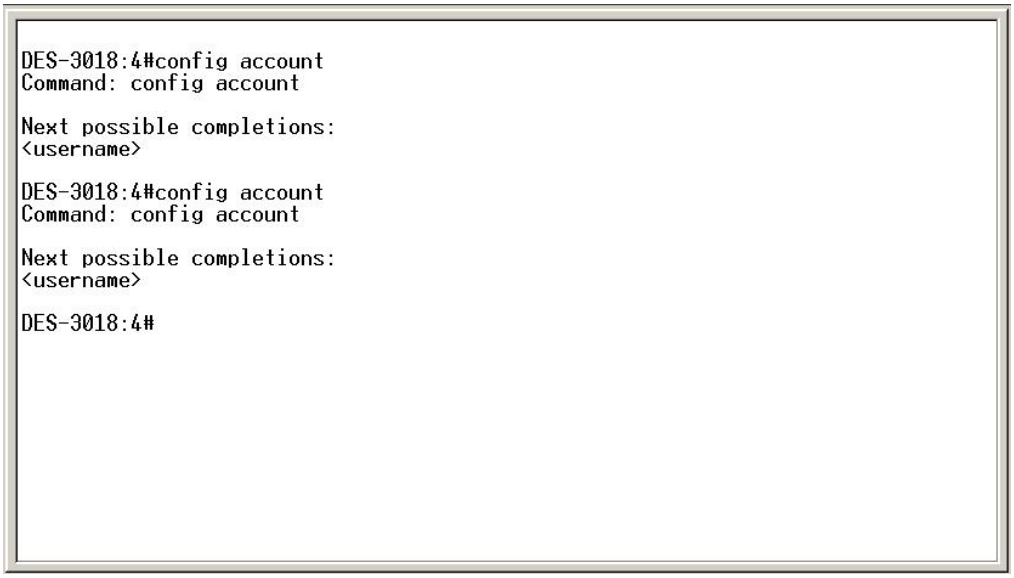

Figure 2-4. Using the Up Arrow to Re-enter a Command

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 user name 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.

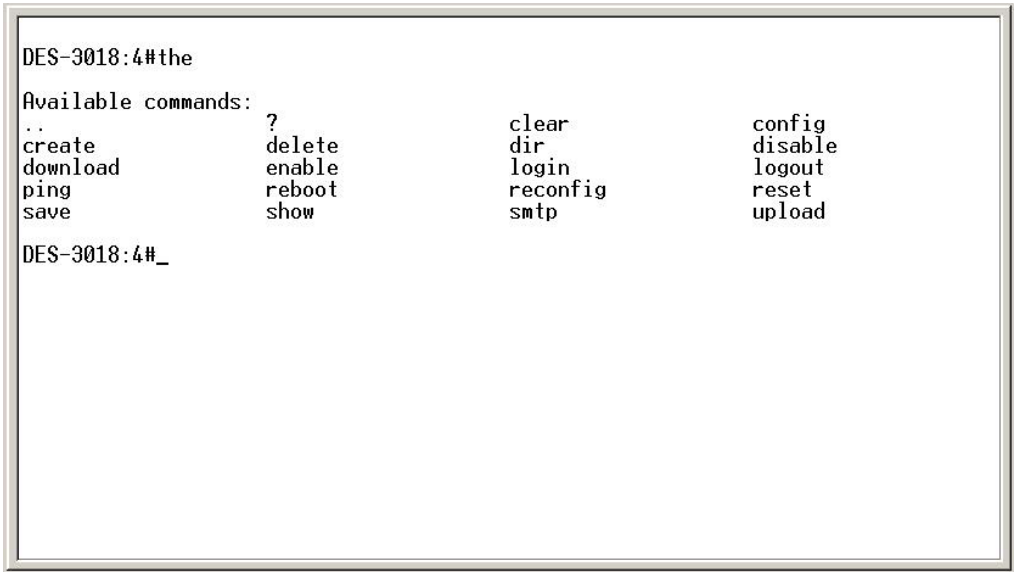

Figure 2-5. The Next Available Commands Prompt

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

```
UserName:
PassWord:

DES-3018:4#show
Command: show

Next possible completions:
802.1p              802.1x              account             acct_client
address_binding     arpentry            auth_client         auth_diagnostics
auth_session_statistics                 auth_statistics     autoconfig
bandwidth_control   command_history     config              cos
cpu_access_profile  dscp_mapping        error               fdb
igmp_snooping       ipif                iproute             lacp_port
link_aggregation    log                 log_save_timing     loopdetect
mac_notification    mirror              multicast           multicast_fdb
packet              port_security       ports               radius
router_ports        scheduling          scheduling_mechanism
serial_port         session             sim                 smtp
snmp                sntp                stp                 switch
syslog              terminal_line       time                traffic
traffic_segmentation                    trusted_host        utilization
vlan

DES-3018:4#_
```

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

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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**config ipif [System] [{ipaddress <network_address> | vlan <vlan_name> | state [enable | disable]} | [description <desc 128> | clear_description} | bootp | dhcp]**
Description	In the above syntax example a VLAN name must be specified in the <vlan_name 32> space and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	**config ipif System ipaddress 10.24.22.5/255.0.0.0 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, an **admin** or a **user** level account must be specified 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	**show multicast_fdb {vlan <vlan_name 32> | mac_address <macaddr>}**
Description	In the above syntax example, either a **VLAN,** or a **MAC address must be specified** to show multicast FDB entries. Do not type the vertical bar.
Example Command	**show multicast_fdb {vlan <vlan_name 32> | mac_address <macaddr>}**

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	**reset {[config | system]}**
Description	In the above syntax example, you have the option to specify **config** or **system**. It is not necessary to specify either optional value, however the effect of the system reset is dependent on which, if any, value is specified. Therefore, with this example there are three possible outcomes of performing a system reset. See the 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 shifts the remaining characters in the line to the left.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Up Arrow	Repeat 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
create account	[admin | user] <username 15>
config account	<username>
delete account	<username> {force_agree}
show account	
show session	
show switch	
show config	[current_config | config_in_nvram]
show serial_port	
config serial_port	{baud_rate [9600 | 19200 | 38400 | 115200] auto_logout [never | 2_minutes | 5_minutes| 10_minutes | 15_minutes]}
enable clipaging	
disable clipaging	
enable telnet	{<tcp_port_number 1-65535>}
disable telnet	
enable web	{<tcp_port_number 1-65535>}
disable web	
save	
reboot	
reset	{[config | system]} {force_agree}
login	
logout	
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.

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 consists 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.

create account	
	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-3026:4#create account admin dlink
Command: create account admin dlink

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

Success.

DES-3026:4#
```

NOTICE: In case of lost passwords or password corruption, please refer to the D-Link website and the White Paper entitled "Password Recovery Procedure", which will guide you through the steps necessary to resolve this issue.

config account	
Purpose	Used to configure user accounts.
Syntax	**config account <username>**
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-3026:4#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-3026:4#
```

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 on the Switch 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-3026:4#show account
Command: show account

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

DES-3026:4#
```

delete account	
Purpose	Used to delete an existing user account.
Syntax	**delete account <username> {force_agree}**
Description	The delete account command deletes a user account that has been created using the **create account** command.
Parameters	<*username*> - Enter the username of the account to be deleted. *force_agree* – Entering this parameter will bypass the “Are you sure?” question and immediately delete the account.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account “System”:

```
DES-3026:4#delete account System
Command: delete account System

Are you sure to delete the last administrator account?(y/n)

Success.

DES-3026:4#
```

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.

show session	
Restrictions	None.

Example usage:

To display the way that the users logged in:

```
DES-3026:4#show session
Command: show session

ID  Login Time            Live Time   From         Level    Name
--  --------------------- ----------- ------------ -------  -------------------
*8  2204/01/26  3:36:27   0:0:20.260  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 information about the Switch.
Syntax	**show switch**
Description	This command displays information about the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch information:

```
DES-3026:4#show switch
Command: show switch

Device Type          : DES-3026 Ethernet Switch
Module 1 Type        : None
Module 2 Type        : None
MAC Address          : DA-10-21-00-00-01
IP Address           : 10.41.44.22 (Manual)
VLAN Name            : default
Subnet Mask          : 255.0.0.0
Default Gateway      : 0.0.0.0
Boot PROM Version : Build 1.01.007
Firmware Version     : Build 4.00.011
Hardware Version     : D1
System Name          : DES-3026_#3
System Location      : 7th_flr_east_cabinet
System Contact       : Julius_Erving_212-555-6666
Spanning Tree        : Disabled
Loopback Detection :
IGMP Snooping        : Disabled
802.1X               : Disabled
TELNET               : Enabled (TCP 23)
WEB                  : Enabled (TCP 80)
RMON                 : Disabled

DES-3026:4#
```

show config	
Purpose	Used to display a list of configuration commands entered into the Switch.
Syntax	**show config [current_config | config_in_nvram]**
Description	This command displays a list of configuration commands entered into the Switch.
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	Only administrator-level users can issue this command.

Example usage:

To view configurations entered on the Switch that were saved to the DRAM:

```
DES-3026:4# show config config_in_nvram
Command: show config config_in_nvram

# BASIC

config serial_port baud_rate 9600 auto_logout never
enable telnet 23
enable web 80
enable clipaging

# STORM

config traffic control 1-16 broadcast disable multicast disable dlf disable
threshold 128

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-3026:4#show serial_port
Command: show serial_port

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

DES-3026:4#
```

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. *auto_logout* - This parameter will allow the user to choose the time the Switch's serial port will be idle before automatically logging out. The user may choose one of the following. ▪ *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-3026:4#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DES-3026:4#
```

enable clipaging

Purpose	Used to pause the scrolling of the console screen when the show 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-3026:4#enable clipaging
Command: enable clipaging

Success.

DES-3026:4#
```

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when the 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 the 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-3026:4#disable clipaging
Command: disable clipaging

Success.

DES-3026:4#
```

enable telnet

Purpose	Used to enable communication with and management of the Switch using the Telnet protocol.
Syntax	**enable telnet {<tcp_port_number 1-65535>}**
Description	This command is used to enable the Telnet protocol on the Switch. The user can specify the TCP 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-3026:4#enable telnet 23
Command: enable telnet 23

Success.

DES-3026:4#
```

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-3026:4#disable telnet
Command: disable telnet

Success.

DES-3026:4#
```

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.
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-3026:4#enable web 80
Command: enable web 80

Success.

DES-3026:4#
```

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-3026:4#disable web
Command: disable web

Success.

DES-3026:4#
```

save	
Purpose	Used to save changes in the Switch's configuration to non-volatile RAM.
Syntax	**save {config | log | all }**
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the Switch's memory each time the Switch is restarted.
Parameters	*config* – Save configuration to NV-RAM. *log* – Save history log. *all* – Save configuration and log.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3026:4#save
Command: save

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

DES-3026:4#
```

reboot	
Purpose	Used to restart the Switch.
Syntax	**reboot {force_agree}**
Description	This command is used to restart the Switch.
Parameters	*force_agree* – Entering this parameter will bypass the "Are you sure?" question and immediately reboot the switch.
Restrictions	None.

Example usage:

To restart the Switch:

```
DES-3026:4#reboot
Command: reboot
Are you sure want to proceed with the system reboot? (y/n)
```

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* – Entering this parameter will bypass the "Are you sure?" question and immediately reset the switch. 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-3026:4#reset config
Command: reset config

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

Success.

DES-3026:4#
```

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 his Username and Password.
Parameters	None.
Restrictions	None.

Example usage:

To initiate the login procedure:

```
DES-3026:4#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-3026:4#logout
```

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. 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. Pinging an IP address without the *times* parameter will ping the target device an infinite amount of times.
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DES-3026:4#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-3026:4#
```

config terminal_line	
Purpose	Used to configure the number of terminal lines produced from the command line interface.
Syntax	**config terminal_line [default | <value 20-80>]**
Description	This command is used to set the number of lines that will be produced by the command line interface of the switch. Users may employ various types of programs to view and configure the Command Line Interface management program for the switch. These programs may have various maximum line display settings other than the standard 24 lines. With this command, users may configure the amount of lines that will be displayed.
Parameters	*default* – Entering this parameter will restore the CLI maximum terminal line settings to its derfault value of 24. *<value 20-80>* - Users may set the number of terminal lines to be displayed for the CLI with this parameter, from 20 to 80 lines.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the terminal lines for 30 lines:

```
DES-3026:4#config terminal_line 30
Command: config terminal_line 30

Success.

DES-3026:4#
```

show terminal_line	
Purpose	Used to display the number of terminal lines to be produced from the Command Line Interface.
Syntax	**show terminal_line**
Description	This command is used to display the number of lines that will be produced by the command line interface of the switch. Users may employ various types of programs to view and configure the Command Line Interface management program for the switch. These programs may have various maximum line display settings other than the standard 24 lines.
Parameters	None.
Restrictions	None.

Example usage:

To display the current terminal lines set for the CLI:

```
DES-3026:4#show terminal_line
Command: show terminal_line

Current terminal line number : 24

DES-3026:4#
```

5

SWITCH PORT COMMANDS

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

Command	Parameters
config ports	config ports [<portlist> | all] {speed [auto | 10_half | 10_full | 100_half | 100_full | {1000_full {[master | slave]}}] | flow_control [enable | disable] | state [enable | disable] | description [<desc 1-128> | clear_description]}
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	**config ports [<portlist> | all] {speed [auto | 10_half | 10_full | 100_half | 100_full | {1000_full {[master | slave]}}] | flow_control [enable | disable] | state [enable | disable] | [description <desc 1-128> | clear_description]}**
Description	This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the <*portlist*> will be affected.
Parameters	<*portlist*> – Specifies a port or range of ports to be configured. *all* – Configure all ports on the Switch. *speed* – Allows the user to set the speed of a port or range of ports, with the addition of one 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 and cannot be set to slower speeds. ▪ *[half | full]* – Configures the specified range of ports as either full- or half-duplex. *[master | slave]* – The *master* and *slave* parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The *master* setting 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 uses loop timing, where the timing comes form a data stream received from the *master*. If one connection is set for *1000 master*, the other side of the connection must be set for *1000 slave*. 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. *state [enable | disable]* – Enables or disables the specified range of ports. *description <desc 128>* - Enter an alphanumeric string of no more than 128 characters to describe a selected port interface. *clear_description* – Enter this command to clear the port description of the selected port(s).
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 and state enabled:

```
DES-3026:4#config ports 1-3 speed 10_full state enable
Command: config ports 1-3 speed 10_full state enable

Success.

DES-3026:4#
```

show ports	
Purpose	Used to display the current configuration of a range of ports.
Syntax	**show ports {<portlist>} {description | err_disabled}**
Description	This command is used to display the current configuration of a range of ports.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed. *description* – Adding this parameter to the command will allow the user to view previously configured descriptions set on various ports on the Switch. *err_disabled* – Used to view information about ports that have had their connection status disabled, for reasons such as STP loopback detection or link down status.
Restrictions	None.

Example usage:

To display the configuration of ports 1-5 on the Switch:

```
DES-3026:4#show ports 1-5
Command: show ports 1-5

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

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

Example usage:

To display port descriptions:

```
DES-3026:4#show ports 1 description
Command: show ports 1 description

Port    Port          Settings                 Connection               Address
        State         Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    Learning
------  --------      ---------------------    ---------------------    --------
1       Enabled       Auto/Enabled             Link Down                Enabled
Description: Accounting

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

Example usage:

To display error ports:

```
DES-3026:4#show ports err_disabled
Command: show ports err_disabled

Port      Port        Connection Status          Reason
          State
------    ---------   --------------------------  -------------
15        Enabled     Err-disabled               Storm Control
          Desc: port15

DES-3026:4#
```

6

NETWORK MANAGEMENT (SNMP) COMMANDS

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

The DES-3026 supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The user may specify which version of the SNMP 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
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 32-bit encryption is added based on the CBC-DES (DES-32) standard

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 33>}
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	

Command	Parameters
create snmp host	<ipaddr> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	{<ipaddr>}
enable rmon	
disable rmon	
create trusted_host	[<ipaddr> | network <network_address>]
delete trusted_host	[<ipaddr> | network <network_address> | all]
show trusted_host	
enable snmp traps	
disable snmp traps	
enable snmp authenticate traps	
disable snmp authenticate traps	
show snmp traps	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>

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.
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 with which the new SNMP user will be associated. *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 a encryption key for authentication and privacy. The key is defined by

create snmp user	
	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: ▪ *<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>* - 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>* - 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-3026:4#create snmp user dlink default encrypted
by_password auth md5 auth_password priv none
Command: create snmp user dlink default encrypted
by_password auth md5 auth_password priv none

Success.

DES-3026:4#
```

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-3026:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-3026:4#
```

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-3026:4#show snmp user
Command: show snmp user

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

Total Entries: 1

DES-3026:4#
```

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.

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

Example usage:

To create an SNMP view:

```
DES-3026:4#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-3026:4#
```

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-3026:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-3026:4#
```

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

show snmp view	
	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-3026:4#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-3026:4#
```

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_name 32*> – An alphanumeric string of up to 32 characters that

create snmp community	
	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-3026:4#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DES-3026:4#
```

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 to delete. 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-3026:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-3026:4#
```

show snmp community	
Purpose	Used to display SNMP community strings configured on the Switch.
Syntax	**show snmp community {<community_string 33>}**
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 33 characters that is used to identify members of an SNMP community. This string is used like a password to give remote

show snmp community	
	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-3026:4#show snmp community
Command: show snmp community

SNMP Community Table

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

Total Entries: 3

DES-3026:4#
```

config snmp engineID	
Purpose	Used to configure a name for the SNMP engine on the Switch.
Syntax	**config snmp engineID <snmp_engineID 10-64>**
Description	The **config snmp engineID** command configures a name for the SNMP engine on the Switch.
Parameters	*<snmp_engineID 10-64>* – An alphanumeric string between 10 and 64 characters 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-3026:4#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DES-3026:4#
```

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-3026:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DES-3026:4#
```

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 with which the new SNMP user will be associated. *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

create snmp group	
	request SNMP messages. ▪ <*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. *write_view* – Specifies that the SNMP group being created has write privileges. ▪ <*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. *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-3026:4#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-3026:4#
```

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 with which the new SNMP user will be associated.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the SNMP group named "sg1".

```
DES-3026:4#delete snmp group sg1
Command: delete snmp group sg1

Success.

DES-3026:4#
```

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-3026:4#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       : Group6
ReadView Name       : ReadView
WriteView Name      : WriteView
Notify View Name    : NotifyView
Security Model      : SNMPv3
Security Level      : authPriv

Group    Name       : Group7
ReadView Name       : ReadView
WriteView Name      : WriteView
Notify View Name    : NotifyView
Security Model      : SNMPv3
Security Level      : authPriv

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

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

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

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

Total Entries: 10

DES-3026:4#
```

create snmp host

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

create snmp host	
	▪ 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-3026:4#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-3026:4#
```

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.
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-3026:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DES-3026:4#
```

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-3026:4#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              public

Total Entries: 2

DES-3026:4#
```

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-3026:4#enable rmon
Command: enable rmon

Success.

DES-3026:4#
```

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-3026:4#disable rmon
Command: disable rmon

Success.

DES-3026:4#
```

create trusted_host	
Purpose	Used to create the trusted host.
Syntax	**create trusted_host [<ipaddr> | network <network_address>]**
Description	The **create trusted_host** command creates the trusted host. The Switch specification of up to ten IP addresses that are allowed to manage the Switch via in-band SNMP or TELNET based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.
Parameters	*<ipaddr>* – The IP address of the trusted host to be created. *network <network_address>* - Users may enter this parameter to configure a trusted network for the device, using an IP address with the appropriate subnet mask.. (ex. If an IP address of 10. 53.13.1/8 was added here, it would constitiute all address from 10.0.0.0 – 10.255.255.255 as trusted IP addresses, or in essence the whole 10 dot network.)
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the trusted host:

```
DES-3026:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DES-3026:4#
```

Example usage:

To create the trusted network:

```
DES-3026:4#create trusted_host  network 11.0.0.0/8
Command: create trusted_host  network 11.0.0.0/8

Success.

DES-3026:4#
```

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

Example usage:

To display the list of trust hosts:

```
DES-3026:4#show trusted_host
Command: show trusted_host

Management Stations

IP Address
----------------------
10.0.0.0/8
11.1.2.3

Total Entries: 1

DES-3026:4#
```

delete trusted_host	
Purpose	Used to delete a trusted host entry made using the **create trusted_host** command above.
Syntax	**delete trusted host [ipaddr <ipaddr> | network <network_address> | all]**
Description	This command is used to delete a trusted host entry made using the **create trusted_host** command above.
Parameters	*<ipaddr>* – The IP address of the trusted host. *network <network_ address>* - Enter the network address with appropriate subnet mask, to be removed from the switch as a trusted network. *all* – Entering this parameter will remove all trusted hosts from the switch.
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-3026:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DES-3026:4#
```

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-3026:4#enable snmp traps
Command: enable snmp traps

Success.

DES-3026:4#
```

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-3026:4#disable snmp traps
Command: disable snmp traps

Success.

DES-3026:4#
```

enable snmp authenticate trap

Purpose	Used to enable SNMP authentication trap support.
Syntax	**enable snmp authenticate trap**

enable snmp authenticate trap	
Description	This command is used to enable SNMP authentication trap support on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To turn on SNMP authentication trap support:

```
DES-3026:4#enable snmp authenticate trap
Command: enable snmp authenticate trap

Success.

DES-3026:4#
```

disable snmp authenticate trap	
Purpose	Used to disable SNMP authentication trap support.
Syntax	**disable snmp authenticate trap**
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-3026:4#disable snmp authenticate trap
Command: disable snmp authenticate trap

Success.

DES-3026:4#
```

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-3026:4#show snmp traps
Command: show snmp traps

SNMP Trap              : Enabled
Authenticate Traps     : Enabled

DES-3026:4#
```

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

Example usage:

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

```
DES-3026:4#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DES-3026:4#
```

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

Example usage:

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

```
DES-3026:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3026:4#
```

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 255 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-3026 Switch**":

```
DES-3026:4#config snmp system_name DES-3026 Switch
Command: config snmp system_name DES-3026 Switch

Success.

DES-3026:4#
```

7

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-3026:4#enable smtp
Command: enable smtp

Success.

DES-3026:4#
```

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-3026:4#disable smtp
Command: disable smtp

Success.

DES-3026:4#
```

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-3026:4#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-3026:4#
```

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-3026:4#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-3026:4# smtp send_testmsg
Command: smtp send_testmsg

Subject: This is a SMTP test.
Content: Hello everybody!!

Sending mail, please wait…

Success.

DES-3026:4#
```

8

DOWNLOAD/UPLOAD COMMANDS

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

Command	Parameters
download	[firmware <ipaddr> <path_filename 64> | configuration <ipaddr> <path_filename 64> {increment}]
upload	[configuration | log] <ipaddr> <path_filename 64>
enable autoconfig	
disable autoconfig	
show autoconfig	

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 <ipaddr> <path_filename 64> | configuration <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* – Download and install new firmware on the Switch from a TFTP server. *configuration* – 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:\3024.had. *increment* – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the Switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To download a firmware file:

```
DES-3026:4#download firmware 10.48.74.121 c:\DES-3026 b08.had
Command: download firmware 10.48.74.121 c:\DES-3026 b08.had

Connecting to server..... Done.
Download firmware.....…… Done. Do not power off!
Please wait, programming flash…….. Done.
Saving current settings to NV-RAM……Done.
Please wait, the switch is rebooting….
```

Example usage:

To download a configuration file:

```
DES-3026:4#download configuration 10.48.74.121 c:\cfg\setting.txt
Command: download configuration 10.48.74.121 c:\cfg\setting.txt

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

DES-3026:4#
```

upload	
Purpose	Used to upload the current switch settings or the Switch history log to a TFTP server.
Syntax	**upload [configuration | log] <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	*configuration* – Specifies that the Switch's current settings will be uploaded to the TFTP server. *log* – Specifies that the Switch history log will be uploaded to the TFTP server. <*ipaddr*> – The IP address of the TFTP server. <*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	Only administrator-level users can issue this command.

Example usage:

To upload a log file:

```
DES-3026:4#upload log 10.48.74.121 c:\cfg\log.txt
Command: upload log 10.48.74.121 c:\cfg\log.txt

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

DES-3026:4#
```

Example usage:

To upload a configuration file:

```
DES-3026:4#upload configuration 10.48.74.121 c:\cfg\log.txt
Command: upload configuration 10.48.74.121 c:\cfg\log.txt

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

DES-3026:4#
```

enable autoconfig	
Purpose	Used to activate the autoconfiguration function for the Switch. This will load a previously saved configuration file for current use.
Syntax	**enable autoconfig**
Description	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: c**onfig ipif System dhcp**). The DHCP server must have the TFTP server IP address and configuration file name, and be configured to deliver this information in the data field of the DHCP reply packet. The TFTP server must be running and have the requested configuration file in its base directory when the request is received from the Switch. Consult the DHCP server and TFTP server software instructions for information on loading a configuration file. If the Switch is unable to complete the autoconfiguration process the previously saved local configuration file present in Switch memory will be loaded. Only administrator-level users can issue this command.

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

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.

Example usage:

To enable autoconfiguration on the Switch:

```
DES-3026:4#enable autoconfig
Command: enable autoconfig

Success.

DES-3026:4#
```

```
DES-3026 Fast Ethernet Switch Command Line Interface

Firmware: Build 2.00.016

Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
UserName:
Password:
DES-3026:4#
DES-3026:4##ROUTE
DES-3026:4#
DES-3026:4#
DES-3026:4#create iproute default 172.18.212.253
Command: create iproute default 172.18.212.253

Success.

DES-3026:4#
DES-3026:4#
```

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

```
DES-3026:4#
DES-3026:4#
DES-3026:4##-------------------------------------------------------------------
DES-3026:4#
DES-3026:4#          End of configuration file for DES-6500
DES-3026:4#
DES-3026:4#-------------------------------------------------------------------
```

disable autoconfig

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

Example usage:

To stop the autoconfiguration function:

```
DES-3026:4#disable autoconfig
Command: disable autoconfig

Success.

DES-3026:4#
```

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.

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

Example usage:

To show the autoconfig configuration set on the Switch:

```
DES-3026:4#show autoconfig
Command: show autoconfig

Autoconfig disabled.

DES-3026:4#
```

9

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

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 port list. The results are separated into three tables, labeled **A**, **B**, and **C** in the window above. Table **A** is relevant to the size of the packets, Table **B** is relevant to the type of packets and Table **C** is relevant to the type of frame associated with these packets.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the packets analysis for port 7:

```
DES-3026:4#show packet ports 7
Command: show packet ports 7

Port number : 7                A                              B
Frame Size       Frame Counts  Frames/sec   Frame Type       Total     Total/sec
------------     ------------  ----------   ----------       -------   ---------
64               3275          10           RX Bytes         408973    1657
65-127           755           10           RX Frames        4395      19
128-255          316           1
256-511          145           0            TX Bytes         7918      178
512-1023         15            0            TX Frames        111       2
1024-1518        0             0
                       C
Unicast RX       152           1
Multicast RX     557           2
Broadcast RX     3686          16

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:

```
DES-3026:4#show error port 3
Command: show error port 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 ports

Purpose	Used to display real-time port utilization statistics.
Syntax	**show utilization ports {<portlist>}**
Description	This command will display the real-time port utilization statistics for the Switch.
Parameters	*ports <portlist>* - Entering this parameter along with a list of ports will display the current utilization of selected ports on the Switch.

show utilization ports

Restrictions	None.

Example usage:

To display the port utilization statistics:

```
DES-3026:4#show utilization ports 1-26
Command: show utilization ports 1-26

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
7       0          0          0
8       0          0          0
9       0          0          0
10      0          0          0
11      0          0          0
12      0          0          0
13      0          0          0
14      0          0          0
15      0          0          0
16      0          0          0
17      0          0          0
18      0          0          0
19      0          0          0
20      0          0          0
21      0          0          0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

show utilization cpu

Purpose	Used to display real-time CPU utilization statistics.
Syntax	**show utilization cpu**
Description	This command will display the real-time CPU utilization statistics for the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the CPU utilization statistics:

```
DES-3026:4#show utilization cpu
Command: show utilization cpu

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

DES-3026:4#
```

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 cleared for statistics.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear the counters:

```
DES-3026:4#clear counters
Command: clear counters

Success.

DES-3026:4#
```

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-3026:4#clear log
Command: clear log

Success.

DES-3026:4#
```

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>* – Enter a value that corresponds to an entry made in the log. Multiple entries may be made in the form of *x*-y, or from a lower number entry to the higher number entry in the log. The smallest number (and therefore the earlier entry) will be first.
Restrictions	None.

Example usage:

To display the Switch history log**:**

```
DES-3026:4#show log index 1-4
Command: show log index 1-4

Index  Time                  Log Text
-----  ----------            ------------------------------------------------------------
4      2005/12/22 03:03:58   Successful login through Console (Username: Anonymous,
                             IP:0.0.0.0, MAC:00-00-00-00-00-00)
3      2005/12/22 03:02:58   Logout through Console (Username: Anonymous, IP:0.0.0.0,
                             MAC:00-00-00-00-00-00)
2      2005/12/22 03:01:28   Successful login through Console (Username: Anonymous,
                             IP:0.0.0.0, MAC:00-00-00-00-00-00)
1      2005/12/22 03:00:01   Logout through Console (Username: Anonymous, IP:0.0.0.0,
                             MAC:00-00-00-00-00-00)

DES-3026:4#
```

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-3026:4#enable syslog
Command: enable syslog

Success.

DES-3026:4#
```

disable syslog

Purpose	Used to disable the system log to be sent to a remote host.
Syntax	**disable syslog**
Description	The **disable syslog** command disables 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-3026:4#disable syslog
Command: disable syslog

Success.

DES-3026:4#
```

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-3026:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-3026:4#
```

create syslog host	
Purpose	Used to create a new syslog host.
Syntax	**create syslog host <index 1-4> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}**
Description	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. *severity* – Severity level indicator. These are described in the following: **Bold** font indicates that the corresponding severity level is currently supported on the Switch. Numerical Severity Code 0 Emergency: system is unusable 1 Alert: action must be taken immediately 2 Critical: critical conditions 3 Error: error conditions **4 Warning: warning conditions** 5 Notice: normal but significant condition **6 Informational: informational messages** 7 Debug: debug-level messages *informational* – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above. *warning* – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above. *all* – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host. *facility* – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values that the Switch currently supports.

create syslog host

Parameters	Numerical Facility Code 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* <*int*> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. *ipaddress* <*ipaddr*> – Specifies the IP address of the remote host where syslog messages will be sent. *state [enable* | *disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create syslog host:

```
DES-3026:4#create syslog host 1 ipaddress 10.53.13.94 severity all facility local0
Command: create syslog host 1 ipaddress 10.53.13.94 severity all facility local0

Success.

DES-3026:4#
```

config syslog host

Purpose	Used to configure the syslog protocol to send system log data to a remote host.
Syntax	**config syslog {host [all <index 1-4>]} {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}**
Description	The **config syslog host** command is used to configure the syslog protocol to send system log information to a remote host.
Parameters	*all* – Specifies that the command will be applied to all hosts. *<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *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 *informational* – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above. *warning* – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above. *all* – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host. *facility* – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values the Switch currently supports.

config syslog host

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

Example usage:

To configure a syslog host:

```
DES-3026:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DES-3026:4#
```

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-3026:4#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3026:4#
```

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-3026:4#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-3026:4#
```

config log_save_timing

Purpose	Used to configure automatic saving of log to Syslog host.
Syntax	**config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]**
Description	The **config log_save_timing** command is used to configure the terms of saving Switch logs to designated hosts.
Parameters	*time_interval <min 1-65535>* – Specifies the minimum interval between saves in minutes. *on_demand* – Specifies that logs are saved when requested by the host receiving the log. *log_trigger* – Specifies that logs are saved when previously configured triggers require the log to be saved to the Syslog host. Use config syslog host command to determine what triggers are used.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure log timing:

```
DES-3026:4#config log_save_timing log_trigger
Command: config log_save_timing log_trigger

Warning: If too many logs are produced, the flash will be worn down
soon!!!
Success

DES-3026:4#
```

show log_save_timing

Purpose	Used to display the method currently used for automatic saving of log to Syslog host.
Syntax	**show_save_timing**
Description	The **show log save timeing** command will display the current configuration of saving Switch logs to designated hosts.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure log timing:

```
DES-3026:4#show log_save_timing
Command: show log_save_timing

Saving log method : on_demand

DES-3026:4#
```

10

SPANNING TREE COMMANDS

The Switch supports 802.1d STP and 802.1w Rapid STP. The spanning tree commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config stp	{maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30> | priority <value 0-61440> | version [rstp | stp] | txholdcount <value 1-10> | fbpdu [enabled | disabled]}
config stp ports	<portlist> {cost [auto | <value 1-200000000>] | priority <value 0-240> | migrate [yes | no] | edge [true | false] | p2p [true | false | auto] | state [enabled | disabled] | fbpdu [enabled | disabled]}
enable stp	
disable stp	
show stp	
show stp ports	{<portlist>}

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

config stp

Purpose	Used to setup STP and RSTP on the Switch.
Syntax	**config stp {maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30> | priority <value 0-61440> | version [rstp | stp] | txholdcount <value 1-10> | fbpdu [enabled | disabled]}**
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch.
Parameters	*maxage <value 6-40>* – The maximum amount of time (in seconds) that the Switch will wait to receive a BPDU packet before reconfiguring STP. The default is 20 seconds. *hellotime <value 1-10>* – The time interval between transmission of configuration messages by the root device. The default is 2 seconds. *forwarddelay <value 4-30>* – The maximum amount of time (in seconds) that the root device will wait before changing states. The default is 15 seconds. *priority <value 0-61440>* – A numerical value between 0 and 61440 that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device. The lower the numerical value, the higher the priority. The default is 32,768. *version [rstp | stp]* - Select the Spanning Tree Protocol version used for the Switch. For IEEE 802.1d STP select *stp*. Select *rstp* for IEEE 802.1w Rapid STP. *txholdcount <value 1-10>* - The maximum number of Hello packets transmitted per interval. Default value = 3. *fbpdu [enabled | disabled]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is enabled.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and hellotime 4:

```
DES-3026:4#config stp maxage 18 hellotime 4
Command: config stp maxage 18 hellotime 4

Success.

DES-3026:4#
```

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	**config stp ports <portlist> {cost [auto | <value 1-200000000>] | priority <value 0-240> | migrate [yes | no] | edge [true | false] | p2p [true | false | auto] | state [enabled | disabled]}**
Description	This command is used to create and configure STP for a group of ports.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *cost* – 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. *priority <value 0-240>* – Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port. Default = 128. *migrate [yes | no] – yes* will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (*yes*) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment. *edge [true | false] – 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*. *state [enabled | disabled]* – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with path cost 19, priority 15, and state enabled for ports 1-5.

```
DES-3026:4#config stp ports 1-5 cost 19 priority 15 state enabled
Command: config stp ports 1-5 cost 19 priority 15 state enabled

Success.

DES-3026:4#
```

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-3026:4#enable stp
Command: enable stp

Success.

DES-3026:4#
```

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-3026:4#disable stp
Command: disable stp

Success.

DES-3026:4#
```

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.

show stp	
Restrictions	None.

Example usage:

To display the status of STP on the Switch:

Status 1: STP enabled with STP compatible version

```
DES-3026:4#show stp
Command: show stp

STP Status       : Enabled
Max Age          : 20
Hello Time       : 2
Forward Delay    : 15
Priority         : 32768
Default Path Cost : 802.1T
STP Version      : STP compatible
TX Hold Count    : 3
Forwarding BPDU  : Enabled

 Designated Root Bridge: 00-54-85-26-05-00
 Root Priority        : 4096
 Cost to Root         : 200004
 Root Port            : 19
 Last Topology Change  : 6sec
 Topology Changes Count: 37
 Protocol Specification: 3
 Max Age              : 20
 Hello Time           : 2
 Forward Delay        : 15
 Hold Time            : 3
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Status 2 : STP disabled

```
DES-3026:4#show stp
Command: show stp

STP Status           : Disabled
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15
Priority             : 32768
Default Path Cost    : 802.1T
STP Version          : RSTP
TX Hold Count        : 3
Forwarding BPDU      : Enabled


DES-3026:4#
```

show stp ports	
Purpose	Used to display the Switch's current per-port group STP configuration.
Syntax	**show stp ports <portlist>**
Description	This command displays the Switch's current per-port group STP configuration.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured.
Restrictions	None.

Example usage:

To display the STP port settings:

```
DES-3026:4#show stp ports
Command: show stp ports

STP Port Information
------------------------------
Port Index          :  1
Connection          : Link Down
State               : Yes
Cost                : *2000000
Priority            : 128
Edge                : No
P2P                 : Yes
Status              : Disabled
Role                : Disabled
Forwarding BPDU     : Enabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

11

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
enable loopdetect	
disable loopdetect	
config loopdetect	[recover_timer [0 | <value 60-1000000>] | interval <value 1-32767>]
show loopdetect	
config loopdetect ports	[<portlist> | all] state [enable | disable]
show loopdetect ports	{<portlist>}

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

enable loopdetect	
Purpose	Used to globally enable the Loopback Detection function on the switch.
Syntax	**enable loopdetect**
Description	This command, along with the **disable loopdetect** command will enable and disable the Loopback Detection function on the switch, without adjusting configurations.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable the Loopback Detection function, globally, on the Switch:

```
DES-3026:4#enable loopdetect
Command: enable loopdetect

Success.

DES-3026:4#
```

disable loopdetect	
Purpose	Used to globally disable the Loopback Detection function on the switch.
Syntax	**disable loopdetect**
Description	This command, along with the **enable loopdetect** command will enable and disable the Loopback Detection function on the switch, without adjusting configurations.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the Loopback Detection function, globally, on the Switch:

```
DES-3026:4#disable loopdetect
Command: disable loopdetect

Success.

DES-3026:4#
```

config loopdetect

Purpose	Used to configure the Loopback Detection function parameters on the switch.
Syntax	**config loopdetect [recover_timer [0 | <value 60-1000000>] | interval <value 1-32767>]**
Description	This command is used to set the parameters for the Loopback Detection function on the switch, without adjusting configurations. The Loopback Detection function is used to identify loops occurring between the Switch and a device that is directly connected to it. The Loopback Detection function will disable a port that has a loop until the anomaly has ceased, and the loopback occurrence will be noted in the Switch's log. Once the loopback problem has stopped, this port will be automatically recovered in a time period that can also be specified by the user.
Parameters	*recover_timer [0 | <value 60-1000000>]*- Enter a time, in seconds that a port will have to wait before being recovered from a Loopback Detection shutdown. The user may set a time between 60 and 1000000 seconds with a default setting of 60 seconds. The user may also enter a time of 0 which means that the port can only be recovered manually by the user. This is done by configuring the **config ports** command and manually enabling these ports. *interval <value 1-32767>* - Enter a time interval, between 1 and 32767 seconds, that CTP (Configuration Testing Protocol) packets will be dispatched from Loopback Detection enabled ports. If this packet is returned, the port will be disabled. The default setting is 10 seconds.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the loopback detection recover timer:

```
DES-3026:4#config loopdetect recover_timer 60
Command: config loopdetect recover_timer 60

Success.

DES-3026:4#
```

Example usage:

To configure the loopback detection CTP packet interval:

```
DES-3026:4#config loopdetect interval 10
Command: config loopdetect interval 10

Success.

DES-3026:4#
```

show loopdetect	
Purpose	Used to display the Loopback Detection function parameters set on the switch.
Syntax	**show loopdetect**
Description	This command will display the loopdetect settings currently set on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the loopback detection parameters:

```
DES-3026:4#show loopdetect
Command: show loopdetect

Loopdetect Global Settings
--------------------------------------------------
Loopdetect Status       : Enabled
Loopdetect Interval     : 10
Recover Time            : 60

DES-3026:4#
```

config loopdetect ports	
Purpose	Used to enable ports on the Switch as loopback detection enabled.
Syntax	**config loopdetect ports [<portlist> | all] state [enable | disable]**
Description	This command enable switch ports for the loopdetect function.
Parameters	*ports* <*portlist*> - Enter a port or range of ports to be set as loopdetect ports. *all* – Using this parameter will configure all ports on the switch as loopback detection ports. *state [enable* | *disable]* – Use this parameter to enable or disable the selected ports as enabled for the loopback detection function.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set ports 1-10 as loopdetect enabled ports:

```
DES-3026:4#config loopdetect ports 1-10 state enable
Command: config loopdetect ports 1-10 state enable

Success.

DES-3026:4#
```

show loopdetect ports	
Purpose	Used to display the Loopback Detection port settings on the switch.
Syntax	**show loopdetect ports {<portlist>}**
Description	This command will display the loopdetect port settings currently set on the switch.
Parameters	*<portlist>* - Enter a port or range of ports to be displayed. Not enetering this parameter will display all ports on the switch.
Restrictions	None.

Example usage:

To display the loopback detection parameters:

```
DES-3026:4#show loopdetect ports 1-5
Command: show loopdetect ports 1-5

Port      Loopdetect State      Loop status
--------  ----------------------  ------------------
1         Enabled                 Normal
2         Enabled                 Normal
3         Enabled                 Normal
4         Enabled                 Normal
5         Disabled                Normal

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

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>
clear fdb	[vlan <vlan_name 32> | port <port> | all]
show multicast_fdb	{vlan <vlan_name 32> | mac_address <macaddr>}
show fdb	{port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}
delete fdb	<vlan_name 32> <macaddr>
config multicast filtering_mode	[forward_unregistered_groups | filter_unregistered_groups]
show multicast 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-3026:4#create fdb default 00-00-00-00-01-02 port 2
Command: create fdb default 00-00-00-00-01-02 port 2

Success.

DES-3026:4#
```

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-3026:4#create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DES-3026:4#
```

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 forwarding table. *[add | delete]* – Add will add the MAC address to the forwarding table. Delete will remove the MAC address from the 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-3026:4#config multicast_fdb default 01-00-5E-00-00-00 add 1
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1

Success.

DES-3026:4#
```

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 5 minutes (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, in seconds.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the fdb aging time:

```
DES-3026:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3026:4#
```

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 deleted from the forwarding table.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DES-3026:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3026:4#
```

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-3026:4#clear fdb all
Command: clear fdb all

Success.

DES-3026:4#
```

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 <vlan_name 32>* – The name of the VLAN on which the MAC address resides. *mac_address <macaddr>* – The MAC address that will be added to the forwarding table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DES-3026:4#show multicast_fdb
Command: show multicast_fdb

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

Total Entries   : 1

DES-3026:4#
```

show fdb	
Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	**show fdb {port <port> | vlan <vlan_name 32> | 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. *<macaddr>* – The MAC address by which the forwarding table will be viewed. *static* – Displays the static MAC address entries. *aging_time* – Displays the aging time for the MAC address forwarding database.
Restrictions	None.

To display the aging time:

```
DES-3026:4#show fdb aging_time
Command: show fdb aging_time

Unicast MAC Address Aging Time = 300

DES-3026:4#
```

Example usage:

To display unicast MAC address table:

```
DES-3026:4#show fdb
Command: show fdb

Unicast MAC Address Ageing Time = 300

VID   VLAN Name   MAC Address        Port    Type
----  ----------  -----------------  ------  ----------
1     default     00-00-39-34-66-9A  10      Dynamic
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 filtering_mode	
Purpose	Used to configure the multicast packet filtering mode for the Switch.
Syntax	**config multicast filtering_mode [forward_unregistered_groups | filter_unregistered_groups]**
Description	This command will configure the multicast packet filtering mode on the Switch.
Parameters	*[forward_unregistered_groups* | *filter_unregistered_groups]* – The user may set the filtering mode to any of these two options.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the multicast filtering mode to filter unregistered groups.

```
DES-3026:4#config multicast filtering_mode filter_unregistered_groups
Command: config multicast filtering_mode filter_unregistered_groups

Success.

DES-3026:4#
```

show multicast filtering_mode	
Purpose	Used to show the multicast packet filtering.
Syntax	**show multicast filtering_mode**
Description	This command will display the current multicast packet filtering mode on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the multicast filtering mode configuration:

```
DES-3026:4#show multicast filtering_mode
Command: show multicast filtering_mode

Multicase Filter Mode : forward_unregistered_groups

DES-3026:4#
```

13

TRAFFIC CONTROL COMMANDS

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

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the **Drop** option of the **Action** field in the window below. The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the Countdown field. If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only method of recovering this port is 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 window 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	[<storm_grouplist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 64-1000000> | time_interval <value 5-30> | countdown [<value 0> | <value 5-30>]}
config traffic control_recover	[<portlist> | all]
config traffic trap	[none | storm_occurred | storm_cleared | both]
show traffic control	{<storm_grouplist>}

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

config traffic control

Purpose	Used to configure broadcast/multicast traffic control.
Syntax	**config traffic control [<storm_grouplist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 64-1000000> | time_interval <value 5-30> | countdown [<value 0> | <value 5-30>]}**
Description	This command is used to configure traffic control.
Parameters	*<storm_grouplist>* – Used to specify a port or 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 unicast traffic control. *action* – Used to configure the action taken when a storm control has been 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

config traffic control	
	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 Shutdown Forever mode and is no longer operational until the user manually resets the port using the **config traffic control_recover** 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/unicast packets, in packets per second (pps), received by the Switch that will trigger the storm traffic control measures. The default setting is 128. *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. • *sec 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. • *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 shutdown forever mode and can only be manually recovered using the **config traffic control_recover** 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 system wide:

```
DES-3026:4#config traffic control all broadcast enable
Command: config traffic control all broadcast enable

Success.

DES-3026:4#
```

config traffic control_recover	
Purpose	Used to configure traffic control recover for any or all ports.
Syntax	**config traffic control_recover [<portlist> | all]**
Description	Configuring a port for traffic control recover will require an administrator to restart the specified ports if storm control shuts down the port or ports. That is, if a storm triggers the action *shutdown* for a port, it will remain in the shutdown even if the threshold falls below the value that triggers the storm control action.
Parameters	<*portlist*> - Used to specify a port or range of ports. *all* – All ports on switches on the switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure traffic control recover for ports 1-6:

```
DES-3026:4#config traffic control_recover 1-6
Command: config traffic control_recover 1-6

Success.

DES-3026:4#
```

config traffic trap	
Purpose	Used to configure traps for traffic control.
Syntax	**config traffic trap [none | storm_occurred | storm_cleared | both]**
Description	Use this to enable traffic storm trap messages.
Parameters	*none* – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism. *storm_occurred* – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. *storm_cleared* – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. *both* – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure traffic control and enable broadcast storm control system wide:

```
DES-3026:4#config traffic trap storm_occurred
Command: config traffic trap storm_occurred

Success.

DES-3026:4#
```

show traffic control	
Purpose	Used to display current traffic control settings.
Syntax	**show traffic control {<storm_grouplist>}**
Description	This command displays the current storm traffic control configuration on the Switch.
Parameters	***<storm_grouplist>*** - Specify a port or range of ports to display. If unspecified, all ports will be displayed.
Restrictions	None.

Example usage:

To display traffic control setting:

```
DES-3026:4#show traffic control
Command: show traffic control

Traffic Storm Control Trap :[None]

Port   Thres  Broadcast  Multicast  Unicast   Action   Count  Time      Shutdown
       hold   Storm      Storm      Storm              down   Interval  Forever
----   -----  ---------  ---------  --------  --------  -----  --------  --------
1      1000   Enabled    Disabled   Disabled  drop      0      5
2      1000   Enabled    Disabled   Disabled  drop      0      5
3      1000   Enabled    Disabled   Disabled  drop      0      5
4      1024   Disabled   Disabled   Disabled  drop      0      5
5      1024   Disabled   Disabled   Disabled  drop      0      5
6      1024   Disabled   Disabled   Disabled  drop      0      5
7      1024   Disabled   Disabled   Disabled  drop      0      5
8      1024   Disabled   Disabled   Disabled  drop      0      5
9      1024   Disabled   Disabled   Disabled  drop      0      5
10     1024   Disabled   Disabled   Disabled  drop      0      5
11     1024   Disabled   Disabled   Disabled  drop      0      5
12     1024   Disabled   Disabled   Disabled  drop      0      5
13     1024   Disabled   Disabled   Disabled  drop      0      5
14     1024   Disabled   Disabled   Disabled  drop      0      5
15     1024   Disabled   Disabled   Disabled  drop      0      5
16     1024   Disabled   Disabled   Disabled  drop      0      5

Total Entries: 16

DES-3026:4#
```

14

QOS COMMANDS

The DES-3000 Series switch supports priority classification for IEEE 802.1p Priority, DiffServ (DSCP) and IP TOS priority. Incoming packets with piority tags are classified into 4 priority queues in the Switch. Priority may also be set according to destination MAC address or Switch port.

For 802.1p Priority, the Switch has 4 priority classes of service. These priority classes of service are numbered from 3 (Class 3) — the highest priority class of service — to 0 (Class 0) — the lowest priority class of service. The eight priority queues specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority classes of service as follows:

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

802.1p priority scheduling is implemented using two types of methods, strict priority and round-robin priority. If no changes are made to the QoS priority scheduling settings the method used is strict priority.

For strict priority-based scheduling, packets residing in the highest priority class of service are transmitted first. Once a strict scheduling is implemented for QoS, the highest class will work in strict mode and the other classes will remain in a weight fair scheduling mode. Higher priority packets always receive preference regardless of the amount of lower priority packets in the buffer and regardless of the time elapsed since any lower priority packets have been transmitted. By default, the Switch is configured to empty the buffer using strict priority.

NOTICE: The default QoS scheduling arrangement is a strict priority schedule which means the switch will consider the highest class of service to have strict scheduling only, while the other queues empty in a round-robin method. See the **config scheduling_mechanism** command in this section for more information regarding this subject.

To use implement round-robin (weighted) priority, the Switch's four priority classes of service can be configured to reduce the buffer in a round-robin fashion - beginning with the highest priority class of service, and proceeding to the lowest priority class of service before returning to the highest priority classes of service.

The weighted-priority based scheduling alleviates the main disadvantage of strict priority-based scheduling – in that lower priority class of service get starved of bandwidth – by providing a minimum bandwidth to all classes of service for transmission. This is accomplished by configuring the maximum number of packets allowed to be transmitted from a given priority class of service and the maximum amount of time a given priority class of service will have to wait before being allowed to transmit its accumulated packets. This establishes a Class of Service (CoS) for each of the Switch's four hardware priority classes of service.

The possible **weight** value range is: 1 to 55 packets.

In networking environments that use alternative QoS protocols, the Switch's CoS can be mapped to accommodate DSCP priority and Type of Service (ToS) priority. CoS can also be mapped to specified destination MAC addresses or ports on the Switch.

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

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

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

config cos mapping

Purpose	Used to configure class of service parameters and mapping for port-based cost of service and mapping for Type of Service (ToS).
Syntax	**config cos mapping port [<portlist> | all] [none | {port_mapping | ethernet [802.1p | mac_mapping] | ip [tos | dscp]}]**
Description	Class of Service is configured to map different QoS priority protocols to the Switch's 4 internal priority queues. CoS mapping can be used to accommodate packets using ToS priority or DSCP priority in their headers. CoS can also be based on destination MAC address. Port-based CoS can be enabled on any port and mapped to one of two priority queues.
Parameters	*mapping* - Specifies CoS mapping based on port (*port <portlist>* or *all*). Port based CoS may be further configured as follows: • *none* – Specifies port-based CoS mapping without additional specification. • *port_mapping* - Enables CoS mapping for the specified ports • *ethernet* – Specifies port-based CoS mapping on selected ports to be *802.1p* priority mapping or MAC address based mapping *mac_mapping*. • *mac_mapping* – Specifiies CoS mapping based on destination MAC address (*destination_addr <macaddr>*). There are four priority levels available for mapping as defined by the class (*class <class_id 0-3>*).

config cos mapping

	• *ip* - Specifies port-based CoS mapping on selected ports to be *tos* or *dscp* mapping. • *tos* – Specifies CoS mapping for Type of Service (ToS) priority. Select the ToS value (*value <value 0 - 7>*) and the class (*class <class_id 0-3>*)
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure CoS to enable port-based CoS mapping:

```
DES-3026:4#config cos mapping port all port_mapping
Command: config cos mapping port all port_mapping

Success

DES-3026:4#
```

show cos mapping

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

Example usage:

To display CoS mapping configuration:

```
DES-3026:4#show cos mapping port 1-3
Command: show cos mapping port 1-3

Port     Port priority      Ethernet_priority        IP_priority
-------------------------------------------------------------------------------
1            off               802.1p                   off
2            off               802.1p                   off
3            off               802.1p                   off

DES-3026:4#
```

config dscp_mapping

Purpose	To configure CoS mapping for DSCP (DiffServ) based priority.
Syntax	**config dscp_mapping dscp_value <0–63> [class <class_id 0-3>]**
Description	This is used to map the 64-level DSCP priority to the 4-level class of service priority used in the Switch.
Parameters	*dscp_value <0 – 63>* - The DSCP priority level being mapped. Each DSCP level must be configured separately to be mapped. *class <class_id 0-3>* - The class of service level being mapped to.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure CoS mapping for DSCP:

```
DES-3026:4#config dscp_mapping dscp_value 1 class 0
Command: config dscp_mapping dscp_value 1 class 0

Success

DES-3026:4#
```

show dscp_mapping

Purpose	To display current DSCP mapping.
Syntax	**show dscp_mapping {dscp_value <value 0-63>}**
Description	Use this to display the CoS priority level currently mapped for DSCP levels.
Parameters	*dscp_value <value 0-63>* - Specify a DSCP value to view the current value mapped to it in the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display current CoS mapping for DSCP:

```
DES-3026:4#show dscp_mapping dscp_value 13
Command: show dscp_mapping dscp_value 13

DSCP    Class
----------------------
13          0

DES-3026:4#
```

config scheduling

Purpose	Used to configure traffic scheduling for each of the Switch's QoS queues.
Syntax	**config scheduling <class_id 0-3> {weight <value 1-55}**
Description	The Switch contains four hardware priority classes of service per device. The Switch's default settings draw down the four hardware classes of service in order, from the highest class (Class 3) to the lowest class (Class 0). Starting with the highest priority class of service (Class 3), the highest priority class of service will transmit all of the packets and empty its buffer before allowing the next lower priority class of service to transmit its packets. The next highest priority class of service will empty before proceeding to the next class of service and so on. Lower priority classes of service are allowed to transmit only if the higher priority classes of service in the buffer are completely emptied. Packets in the higher priority classes of service are always emptied before any in the lower priority classes of service regardless of latency or volume of the lower priority classes of service. The default settings for QoS scheduling employ this strict priority scheme to empty priority classes of service. The **config scheduling** command can be used to specify the round robin rotation by which these four hardware priority classes of service are reduced. The **weight** parameter allows specification of the maximum number of packets a given priority classes of service can transmit before allowing the next lowest priority queue to begin transmitting its packets. A value between 0 and 55 packets can be

config scheduling

	specified. For example, if a value of 5 is specified, then the highest priority class of service (queue 3) will be allowed to transmit 5 packets. Then the next lower priority class of service (queue 2) will be allowed to transmit 5 packets, and so on, until all of the classes of service have transmitted 5 packets. The process will then repeat.
Parameters	*<class_id>* – Specifies which of the four priority classes of service to which the **config scheduling** command will be applied. The four priority classes of service are identified by number – from 0 to 3 – with class 3 being the highest priority. *weight <value 1-55>* – Specifies the maximum number of packets the above specified priority class of service will be allowed to transmit before allowing the next lowest priority classes of service to transmit its packets. A value between 1 and 55 packets can be specified. The default value is per class is: Class Weight 0 1 1 2 2 4 3 8
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure traffic scheduling:

```
DES-3026:4#config scheduling 3 weight 15
Command: config scheduling 3 weight 15

Success.

DES-3026:4#
```

show scheduling

Purpose	Used to display the currently configured traffic scheduling on the Switch.
Syntax	**show scheduling**
Description	The **show scheduling** command displays the current configuration for the maximum number of packets (**weight**) value assigned to the four priority classes of service on the Switch. The Switch will empty the four hardware classes of service in order, from the highest priority (class 3) to the lowest priority (class 0).
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```
DES-3026:4# show scheduling

Command: show scheduling

QOS Output Scheduling

Class ID       Weight
---------- ----------
Class-0         1
Class-1         2
Class-2         4
Class-3        15

DES-3026:4#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the four hardware classes of service available on the Switch.
Syntax	**config 802.1p user_priority <priority 0-7> <class_id 0-3>**
Description	The **config 802.1p user_priority** command is used to configure the way the Switch will map an incoming packet, based on its 802.1p user priority tag, to one of the four hardware priority classes of service available on the Switch. The Switch's default is to map the incoming 802.1p priority values to the four hardware classes of service according to the following chart: 802.1p Value — Switch Priority Queue 0 — 1 1 — 0 2 — 0 3 — 1 4 — 2 5 — 2 6 — 3 7 — 3
Parameters	*<priority 0-7>* – Specifies to which of the eight 802.1p priority values (0 through 7) to map to one of the Switch's hardware priority classes of service (<class_id>, 0 through 3). *<class_id 0-3>* – Specifies to which of the Switch's hardware priority classes of service the 802.1p priority value (specified above) will be mapped.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1 user priority on the Switch:

```
DES-3026:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-3026:4#
```

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 classes of service.
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 classes of service.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1p user priority:

```
DES-3026:4# 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-3026:4#
```

config 802.1p default_priority	
Purpose	Used to assign an 802.1p priority tag to an incoming untagged packet that has no 802.1p priority tag.
Syntax	**config 802.1p default_priority [<portlist> | all] <priority 0-7>**
Description	The **config 802.1p default_priority** command allows specification of the 802.1p priority value an untagged, incoming packet will be assigned before being forwarded to its destination.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *all* – Specifies that the **config 802.1p default_priority** command will be applied to all ports on the Switch. *<priority 0-7>* – Specifies the 802.1p priority value that an untagged, incoming packet will be given before being forwarded to its destination.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the Switch:

```
DES-3026:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3026:4#
```

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 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 viewed.
Restrictions	None.

Example usage:

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

```
DES-3026:4# show 802.1p default_priority
Command: show 802.1p default_priority

Port    Priority
-------  -----------
   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
  20       0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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 (WRR)** and a **Strict** mechanism for emptying the priority classes of service of the QoS function. The Switch

config scheduling_mechanism	
	contains four hardware priority classes of service. Incoming packets must be mapped to one of these four hardware priority classes of service. This command is used to specify the rotation by which these four hardware priority classes of service are emptied. The Switch's default is to empty the four priority classes of service in order – from the highest priority class of service (queue 3) to the lowest priority class of service (queue 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority class of service to transmit its packets. Lower classes of service will be pre-empted from emptying its queue if a packet is received on a higher class of service. The packet that was received on the highest 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. Other classes of service will follow weight fair scheduling. *weight_fair* – Entering the weight fair parameter indicates that the priority classes of service will empty packets in a weighted round-robin (***WRR***) 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 COS queue:

```
DES-3026:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DES-3026:4#
```

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 mechanism in use on the Switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show the scheduling mechanism:

```
DES-3026:4#show scheduling_mechanism
Command: show scheduling_mechanism

Scheduling  Mechanism : strict

DES-3026:4#
```

config bandwidth_control	
Purpose	Used to configure bandwidth control on a 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 by-port basis.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured for bandwidth control. *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 packet limit, in kbps, 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 transmitted by the above specified ports. ▪ *<value 64-1024000>* – Specifies the packet limit, in kbps, that the above ports will be allowed to transmit.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DES-3026:4#config bandwidth_control 1-10 rx_rate 100000 tx_rate 100000
Command: config bandwidth_control 1-10 rx_rate 100000 tx_rate 100000

Success.

DES-3026:4#
```

show bandwidth_control	
Purpose	Used to display the bandwidth control configuration on the Switch.
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. Using this command without adding a portlist entry will show the bandwidth control for all ports in the Switch stack.
Restrictions	None.

Example usage:

To display bandwidth control settings:

```
DES-3026:4#show bandwidth_control 1-12
Command: show bandwidth_control 1-12

Bandwidth Control Table

Port    RX Rate (kbit/sec)  TX_RATE (kbit/sec)
----    ------------------  ------------------
1       100000              100000
2       100000              100000
3       100000              100000
4       100000              100000
5       100000              100000
6       100000              100000
7       100000              100000
8       100000              100000
9       100000              100000
10      100000              100000
11      no_limit            no_limit
12      no_limit            no_limit

DES-3026:4#
```

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 [class <class_id 0 | 3>] [<portlist> | all]**
Description	Use this command to configure port-to-class CoS mapping. Port mapping must first be enabled using the command **config cos mapping port <portlist> port_mapping** on the ports before this can be configured.
Parameters	*class [0 | 3]* – Specifies to which of the Switch's hardware priority classes of service value will be mapped for the port or ports. There are two classes available for port COS mapping. *<portlist>* – Specifies a port or range of ports to be configured. *all* – Specifies that the mapping will be applied to all ports on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure CoS port mapping for a range of ports:

```
DES-3026:4#config cos port_mapping class 0 1-4
Command: config cos port_mapping class 0 1-4

Success

DES-3026:4#
```

show cos port_mapping

Purpose	Used to display the current Switch port CoS mapping configuration.
Syntax	**show cos port_mapping {port <portlist>}**
Description	Use this command to view the current configuration for port-to-class CoS settings for any or all ports.
Parameters	*port <portlist>* – Specifies a port or range of ports to view settings. If no ports

show cos port_mapping	
	are specified, all ports are listed.
Restrictions	None.

Example usage:

To view CoS port mapping for a range of ports:

```
DES-3026:4#show cos port_mapping ports 1-2
Command: show cos port_mapping ports 1-2

Port  Priority
----  --------
 1      0
   0

DES-3026:4#
```

config cos mac_mapping destination_addr	
Purpose	Used to map the destination MAC address of an 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	Use this command to map a static destination MAC address to one of the four hardware queues on the Switch. The static MAC address must exist in the Switch forwarding database in order to use this command. See the command **create fdb <vlan_name 32> <macaddr> port <port>** for an example of how to create a static entry in the FDB.
Parameters	*<macaddr>* - Specify the static destination MAC address to be mapped to a harware queue. *class <class_id 0-3>* – Specify the hardware queue to which the MAC address is mapped.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To map a static MAC address to hardware queue 3:

```
DES-3026:4#config cos mac_mapping destination_addr 01-00-D6-E4-FF-05 class 3
Command: config cos mac_mapping destination_addr 01-00-D6-E4-FF-05 class 3

Success.

DES-3026:4#
```

show cos mac_mapping	
Purpose	Used to display MAC address CoS mapping configuration.
Syntax	**show cos mac_mapping { destination_addr < macaddr > }**
Description	Use this command to view a single entry or all entries configured for CoS MAC address mapping.
Parameters	*destination_addr* < *macaddr* > - Specify a static MAC address entry to view the current CoS mapping configuration. If no entry specified, all MAC

show cos mac_mapping	
	mapping entries are listed.
Restrictions	None.

Example usage:

To view the current CoS mapping for static MAC addresses:

```
DES-3026:4#show cos mac_mapping
Command: show cos mac_mapping

MAC Address         Class
----------------------------------
01-00-D6-E4-FF-05     3

DES-3026:4#
```

config cos tos value	
Purpose	Used to map the Type of Service (ToS) value in the IP header of incoming packets to one of the four hardware queues available on the switch.
Syntax	**config cos tos value <value 0-7> [class <class_id 0-3>]**
Description	Use this command to map ToS priority value in the IP header of an incoming packet to one of the hardware queues on the Switch.
Parameters	*<value 0-7>* - Specifies the ToS value in the IP header to be mapped. *class <class_id 0-3>* - Specify the hardware queue to which the ToS value is mapped.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To map a ToS priority value 3 to a hardware queue 2 for incoming packets with ToS information:

```
DES-3026:4#config cos tos value 3 class 2
Command: config cos tos value 3 class 2

Success

DES-3026:4#
```

show cos tos	
Purpose	Used to display the current ToS mapping configuration on the Switch.
Syntax	**show cos tos {value <value 0-7>}**
Description	Use this command to view ToS mappipng for any or all ToS priority values.
Parameters	*value <value 0-7>* - Specifies a ToS value in order to view CoS mapping configuration for that value. If no value is specified, all eight ToS mapped values are listed.
Restrictions	None.

Example usage:

To show the CoS to ToS mapping.

```
DES-3026:4#show cos tos
Command: show cos tos

TOS value    Class
---------------------------
 0           0
 1           0
 2           0
 3           2
 4           0
 5           0
 6           0
 7           0

DES-3026::4#
```

15

TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows you to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied. The traffic segmentation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config traffic_segmentation	[<portlist>] forward_list [null | <portlist>]
show traffic_segmentation	{<portlist>}

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

config traffic_segmentation

Purpose	Used to configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation [<portlist>] forward_list [null | <portlist>]**
Description	The **config traffic_segmentation** command is used to configure traffic segmentation on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured for traffic segmentation. *forward_list* – Specifies a port or 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-3026:4#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DES-3026:4#
```

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-3026:4#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port  Forward Portlist
----  ----------------------------
1     11-15
2     11-15
3     11-15
4     11-15
5     11-15
6     11-15
7     11-15
8     11-15
9     11-15
10    11-15
11    1-26
12    1-26
13    1-26
14    1-26
15    1-26
16    1-26
17    1-26
18    1-26
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

16

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.
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, the user can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	*port <port>* – This specifies the Target port (the port where mirrored packets will be sent). *[add | delete]* – Specify whether to add or delete source ports, which will be specified using the following parameter. *source ports* – The port or ports being mirrored. This cannot include the Target port. ▪ *<portlist>* – This specifies a 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. *rx* - Allows the mirroring of only packets sent from (flowing from) 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 configure the mirror ports:

```
DES-3026:4# config mirror port 10 add source ports 1-5 both
Command: config mirror port 10 add source ports 1-5 both

Success.

DES-3026:4#
```

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 a mirror entry to be enabled on the Switch, without modifying the port mirroring configuration.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable mirroring configurations:

```
DES-3026:4#enable mirror
Command: enable mirror

Success.

DES-3026:4#
```

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 a mirror entry to be disabled on the Switch, without modifying the port mirroring configuration.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DES-3026:4#disable mirror
Command: disable mirror

Success.

DES-3026:4#
```

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-3026:4#show mirror
Command: show mirror

Current Settings
Mirror Status     : enable
Target Port       : 2
Mirrored Port
                  RX :
                  TX :


DES-3026:4#
```

17

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>}
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> {[add [tagged | untagged] | delete] <portlist>}
show vlan	{<vlan_name 32>}

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>}**
Description	This command allows the creation of a VLAN on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN to be created. *tag <vlanid 2-4094>* – The VLAN ID of the VLAN to be created. Allowed values = 2-4094. VLAN 1 is reserved for the default VLAN set originally on the Switch.
Restrictions	Each VLAN name can be up to 32 characters. Only administrator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DES-3026:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DES-3026:4#
```

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-3026:4#delete vlan v1
Command: delete vlan v1

Success.

DES-3026:4#
```

config vlan	
Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan <vlan_name 32> {[add [tagged | untagged] | delete] <portlist>}**
Description	This command allows the user to add or delete ports to the port list of a previously configured VLAN. Additional ports may be specified as tagging or untagging. The default is to assign the ports as untagged.
Parameters	*<vlan_name 32>* – The name of the VLAN to which to add ports. *add* – Specifies to add ports to a previously created vlan. *delete* - Specifies to delete ports to a previously created vlan. *tagged* – Specifies the additional ports as tagged. *untagged* – Specifies the additional ports as untagged. *<portlist>* – A port or range of ports to be added to or deleted from the VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3026:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DES-3026:4#
```

show vlan	
Purpose	Used to display the current VLAN configuration on the Switch
Syntax	**show vlan {<vlan_name 32>}**
Description	This command displays summary information about each VLAN including the VLAN ID, VLAN name, the Tagging/Untagging status, and the Member/Non-member status of each port that is a member of the VLAN.
Parameters	*<vlan_name 32>* – The VLAN name of the VLAN for which to display a summary of settings.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DES-3026:4#show vlan
Command: show vlan

VID              : 1                    VLAN Name      : default
VLAN TYPE        : static
Member ports     : 1-26
Static ports     : 1-26
Tagged ports     :
Untagged ports   : 1-26

Total Entries : 1

DES-3026:4#
```

18

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 1-3> {type [lacp | static]}
delete link_aggregation	group_id <value 1-3>
config link_aggregation	group_id <value 1-3> {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 1-3> | 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 1-3> {type [lacp | static]}**
Description	This command will create a link aggregation group with a unique identifier.
Parameters	*<value 1-3>* – Specifies the group ID. The Switch allows up to 3 link aggregation groups to be configured. The group number identifies each of the groups. **group_id 3** is designed for the uplink modules only (the last two ports on the Switch (9-10, 17-18, 25-26) and can only be configured for them. *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 trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DES-3026:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DES-3026:4#
```

delete link_aggregation group_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value 1-3>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	*<value 1-3>* – Specifies the group ID. The Switch allows up to 3 link aggregation groups to be configured. The group number identifies each of the groups. **group_id 3** is designed for the uplink modules only (the last two ports on the Switch (9-10, 17-18, 25-26) and can only be configured for them.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DES-3026:4#delete link_aggregation group_id 1
Command: delete link_aggregation group_id 1

Success.

DES-3026:4#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-3> {master_port <port> | ports <portlist> | state [enable | disable]}**
Description	This command allows configuration of a link aggregation group that was created with the **create link_aggregation** command above.
Parameters	*<value 1-3>* – Specifies the group ID. The Switch allows up to 3 link aggregation groups to be configured. The group number identifies each of the groups. **group_id 3** is designed for the uplink modules only (the last two ports on the Switch (9-10, 17-18, 25-26) and can only be configured for them. *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. Ports may be listed in only one port aggregation group, that is, link aggregation groups may not overlap. *state [enable | disable]* – Allows the user to enable or disable the specified link aggregation group.
Restrictions	Only administrator-level users can issue this command. Link aggregation groups may not overlap and must be contained on a single switch.

Example usage:

To define a load-sharing group of ports, group-id 1,master port 5 of module 1 with group members ports 5-7 plus port 9:

```
DES-3026:4#config link_aggregation group_id 1 master_port 5 ports 5-7,9
Command: config link_aggregation group_id 1 master_port 5 ports 5-7,9

Success.

DES-3026:4#
```

NOTE: group_id 3 is designed for the uplink modules only (the last two ports on the Switch (DES-3010F/FL/G ports 9-10, DES-3018 ports 17-18, DES-3026 ports 25-26) and can only be configured for them. Any other attempt at configuring group_id 3 with standard 10/100 Mbps ports will result in a configuration error.

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 to 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-3026:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3026:4#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the Switch.
Syntax	**show link_aggregation {group_id <value 1-3> | algorithm}**
Description	This command will display the current link aggregation configuration of the Switch.
Parameters	*<value 1-3>* – Specifies the group ID. The Switch allows up to 3 link aggregation groups to be configured. The group number identifies each of the groups. **group_id 3** is designed for the uplink modules only (the last two

show link_aggregation	
	ports on the Switch (9-10, 17-18, 25-26) and cannot be viewed here.
	algorithm – Displays the link aggregation algorithm in use on the Switch.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DES-3026:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = mac_source

Group ID       : 1
Type           : TRUNK
Master Port    : 5
Member Port    : 5-7
Active Port    :
Status         : Disabled
Flooding Port  : 0

DES-3026:4#
```

Example Usage:

To display the link aggregation algorithm set on the switch.

```
DES-3026:4#show link_aggregation algorithm
Command: show link_aggregation algorithm

Link Aggregation Algorithm = mac_source

DES-3026:4#
```

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 range of ports to be configured for LACP. *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).

config lacp_ports	
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DES-3026:4#config lacp_port 1-6 mode active
Command: config lacp_port 1-6 mode active

Success.

DES-3026:4#
```

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 range of ports that will be viewed.
Restrictions	None.

Example usage:

To display LACP port mode settings:

```
DES-3026:4#show lacp_port 1-11
Command: show lacp_port 1-11

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

DES-3026:4#
```

19

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] | [description <desc 128> | clear_description} | bootp | dhcp]
show ipif	

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

config ipif	
Purpose	Used to configure the System IP interface.
Syntax	**config ipif [System] [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable] | [description <desc 128> | clear_description} | bootp | dhcp]**
Description	This command is used to configure the System IP interface on the Switch.
Parameters	*System* - The IP interface name to be configured. The default IP Interface name on the Switch is "System". All IP interface configurations done will be executed through this interface name. *<network_address>* – IP address and netmask of the IP interface to be created. The address and mask information may be specified by using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16). *<vlan_name 32>* – The name of the VLAN corresponding to the System IP interface. *state [enable | disable]* – Used to enable or disable the IP interface. *description <desc 128>* - Enter an alphanumeric string of up to 128 characters to identify the IP interface being configured here. *clear_description* – Enter this parameter to remove a previously entered description for this 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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DES-3026:4#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DES-3026:4#
```

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-3026:4#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    : 1-26
Description     : MyNet

DES-3026:4#
```

20

IP-MAC BINDING COMMANDS

The IP-MAC 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 | disable] allow_zeroip [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	

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

create address_binding ip_mac ipaddress	
Purpose	Used to create an IP-MAC address binding entry.
Syntax	**create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}**
Description	This command will create an IP-MAC address binding entry.
Parameters	*<ipaddr>* - The IP address of the device to be bound to the MAC address stated below. *mac_address <macaddr>* - The MAC address of the device to be bound to the IP address stated above. *ports [<portlist> | all]* – The port or ports bound to the IP address and MAC address stated above.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an IP-MAC address binding entry on the Switch:

```
DES-3026:4#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-3026:4#
```

config address_binding ip_mac ipaddress	
Purpose	Used to configure a previously set IP-MAC address binding entry.
Syntax	**config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] }**
Description	This command will configure an IP-MAC address binding entry.
Parameters	*<ipaddr>* - The IP address of the device to be bound to the MAC address stated below. *mac_address <macaddr>* - The MAC address of the device to be bound to the IP address stated above. *ports [<portlist> | all]* – The port or ports bound to the IP address and MAC address stated above.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure a IP to MAC address binding entry on the Switch:

```
DES-3026:4#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-3026:4#
```

config address_binding ip_mac ports	
Purpose	Used to enable ports on the Switch to be configured for IP-MAC address binding.
Syntax	**config address_binding ip_mac ports [<portlist> | all] state [enable | disable] allow_zeroip [enable | disable]**
Description	This command will configure ports as enabled or disabled for the IP-MAC address binding function.
Parameters	*<portlist>* – Specifies a port or range of ports to be enabled or disabled for IP-MAC address binding. *all* – Specifies all ports on the Switch are to be enabled or disabled for IP-MAC address binding. *state - [enable | disable]* – Enables or disables the specified range of ports for IP-MAC address binding. *allow_zeroip [enable | disable]* - The **allow_zeroip** parameter is used to allow ARP packets entrance to the Switch when these packets have an IP address of 0.0.0.0, regardless of whether or not the 0.0.0.0 IP address is set in the IP-MAC Binding table. When the **allow_zeroip** parameter is set to *disable*, ARP packets containing the 0.0.0.0 IP address are dropped. Please note that this function does not affect the IP-MAC Binding ACL Mode.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure port 2 to be enabled for IP-MAC address bindings:

```
DES-3026:4#config address_binding ip_mac ports 2 state enable allow_zeroip enable
Command: config address_binding ip_mac ports 2 state enable allow_zeroip enable

Success.

DES-3026:4#
```

show address_binding

Purpose	Used to display IP-MAC address binding entries.
Syntax	**show address_binding [ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]**
Description	This command will display IP-MAC address binding entries set on the Switch.
Parameters	*ip_mac* – Enter this parameter to view an IP-MAC address binding entry by entering the following: • *all* – Choose this parameter to view all IP-MAC binding entries. • *ipaddress* <*ipaddr*> - The IP address of the device where the IP-MAC binding is made. • *mac_address* <*macaddr*> - The MAC address of the device where the IP-MAC binding is made. *blocked* – Choose this parameter to view the IP-MAC address blocked binding entries by entering one of the following choices to view it by: • *all* – Choose this parameter to view all IP-MAC binding blocked entries. • *vlan_name* <*vlan_name*> - Enter the VLAN name for which to view the IP-MAC address binding blocked entry. This entry must be made with the *mac_address* listed below to view this blocked entry. • *mac_address* <*macaddr*> - The MAC address of the device where the IP-MAC blocked binding is made. This entry is to be made with the vlan name listed above to view this blocked entry. *ports* – Enter this parameter to view the ports which are enabled for IP-MAC binding.
Restrictions	None.

Example usage:

To show IP-MAC binding entries on the switch:

```
DES-3026:4#show address_binding ip_mac ipaddress 10.1.1.8
mac_address 00-00-00-00-00-12
Command: show address_binding ip_mac ipaddress 10.1.1.8
mac_address 00-00-00-00-00-12

Enabled ports: 2

IP Address       MAC Address
---------------  -----------------
10.1.1.8         00-00-00-00-00-12

Total entries : 1

DES-3026:4#
```

delete address_binding

Purpose	Used to delete an IP-MAC address binding entry.
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 address binding entries. Two methods of deletion can be applied. *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 IP-MAC address binding entries, toggle *all.*
Parameters	*ip_mac* – Select this parameter to delete a specific IP-MAC address binding entry by entering the following IP-MAC address binding information. • *ipaddress* <*ipaddr*> - Enter the IP address of the device where the IP-MAC address binding is made. This entry will be used in conjunction with the following MAC address to identify the binding entry to be deleted. • <*macaddr*> The MAC address of the device where the IP-MAC address binding entry is made. This entry will be used in conjunction with the previous IP address to identify the binding entry to be deleted. • *all* - Entering this parameter will delete all IP-MAC address binding entries. *blocked* – Entering this parameter will specify that the user wishes to delete a particular blocked IP-MAC address entry, defined by entering the following parameters. • *all* - Entering this parameter will delete all blocked IP-MAC address binding entries. • *vlan_name* <*vlan_name*> Enter the VLAN name of the VLAN that is bound to a MAC address which the user wishes to delete. This entry must be implemented with the following parameter to specify the entry to be deleted. • <*macaddr*> The MAC address of the device where the blocked IP-MAC address binding is made. This entry will be used in conjunction with the previous VLAN Name to identify the binding entry to be deleted.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an IP-MAC Binding on the switch:

```
DES-3026:4#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-3026:4#
```

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-3026:4#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DES-3026:4#
```

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-3026:4#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DES-3026:4#
```

21

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-3026:4#enable mac_notification
Command: enable mac_notification

Success.

DES-3026:4#
```

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-3026:4#disable mac_notification
Command: disable mac_notification

Success.

DES-3026:4#
```

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 notificiation 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-3026:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DES-3026:4#
```

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 notificiation is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist>* - Specify 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-3026:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-3026:4#
```

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-3026:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State        : Enabled
Interval     : 1
History Size : 1

DES-3026:4#
```

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-3026:4#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
```

22

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>
enable igmp snooping	{forward_mcrouter_only}
disable igmp snooping	
show igmp snooping	{vlan <vlan_name 32>}
show igmp snooping group	{vlan <vlan_name 32>}
show router_ports	{vlan <vlan_name 32>} {[static | dynamic]}

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

config igmp_snooping

Purpose	Used to configure IGMP snooping on the Switch.
Syntax	**config igmp_snooping [vlan_name <vlan_name 32> | all] {host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state [enable | disable] | fast_leave [enable | disable]}**
Description	This command allows the user to configure IGMP snooping on the Switch.
Parameters	*vlan_name <vlan_name 32>* – The name of the VLAN for which IGMP snooping is to be configured. *all* – Selecting this parameter will configure IGMP for all VLANs on the Switch. *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. *leave_timer <sec 1-16711450>* – Leave timer. The default is 2 seconds. *state [enable | disable]* – Allows the user to enable or disable IGMP snooping for the specified VLAN. *fast_leave [enable | disable]* – This parameter allows the user to enable the *fast leave* function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DES-3026:4#config igmp_snooping vlan_name default host_timeout 250 state enable
Command: config igmp_snooping vlan_name default host_timeout 250 state enable

Success.

DES-3026:4#
```

config igmp_snooping querier

Purpose	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping.
Syntax	**config igmp_snooping querier [vlan_name <vlan_name 32> | 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	This command configures IGMP snooping querier.
Parameters	*vlan_name* <*vlan_name 32*> – The name of the VLAN for which IGMP snooping querier is to be configured. *all* – Selecting this parameter will configure IGMP for all VLANs on the Switch. *query_interval* <*sec 1-65535*> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. *max_response_time* <*sec 1-25*> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds. *robustness_variable* <*value 1-255*> – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. Users may wish to increase this value if a subnet is expected to be lossy. *last_member_query_interval* <*sec 1-25*> – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The user may 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 [enable* | *disable]* – Allows the Switch to be specified as an IGMP Querier or Non-querier.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DES-3026:4#config igmp_snooping querier vlan_name default query_interval 125 state enable
Command: config igmp_snooping querier vlan_name default query_interval 125 state enable

Success.

DES-3026:4#
```

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 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]* – Specify whether to add or delete ports defined in the following parameter *<portlist>*, to the router port function. *<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-3026:4#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DES-3026:4#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**enable igmp_snooping {forward_mcrouter_only}**
Description	This command allows you 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-3026:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3026:4#
```

disable igmp_snooping

Purpose	Used to disable IGMP snooping on the Switch.
Syntax	**disable igmp_snooping**
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	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DES-3026:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3026:4#
```

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-3026:4#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State    : Disabled
Multicast router Only         : Disabled

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

Total Entries: 1

DES-3026:4#
```

show igmp_snooping group

Purpose	Used to display the current IGMP snooping group configuration on the Switch.
Syntax	**show igmp_snooping group {vlan <vlan_name 32>}**
Description	This command will display the current IGMP snooping group configuration on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view IGMP snooping group configuration information.
Restrictions	None.

Example usage:

To show IGMP snooping group:

```
DES-3026:4#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   : 3,4

Total Entries   : 1

DES-3026:4#
```

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]}**
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.
Restrictions	None.

Example usage:

To display the router ports.

```
DES-3026:4#show router_ports

Command: show router_ports

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

Total Entries: 1

DES-3026:4#
```

23

CPU ACL FILTERING COMMANDS

The DES-3000 switch series implements Access Control Lists for the CPU that enable the Switch to deny network access to specific devices or device groups based on IP settings, MAC address and packet content settings.

Access profiles allow users to establish criteria to determine whether or not the Switch will forward packets to the CPU based on the information contained in each packet's header. These criteria can be specified on a VLAN-by-VLAN basis.

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

create cpu access_profile profile_id 1 ip source_ip_mask 255.255.255.0

Here we have created an access profile that will examine the IP field of each frame received by the Switch. Each source IP address the Switch finds will be combined with the **source_ip_mask** with a logical AND operational method. The **profile_id** parameter is used to give the access profile an identifying number – in this case, **1**. The **deny** parameter instructs the Switch to filter any frames that meet the criteria.

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

Now that an access profile has been created, add the criteria the Switch will use to decide if a given frame should be forwarded or filtered. Here, we want to filter any packets that have an IP source address between 10.42.73.0 and 10.42.73.255:

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

Here we use the **profile_id 1** which was specified when the access profile was created. The **add** parameter instructs the Switch to add the criteria that follows to the list of rules that are associated with access profile 1. For each rule entered into the access profile, users can assign an **access_id** that both identifies the rule and establishes a priority within the list of rules. A lower **access_id** gives the rule a higher priority. In case of a conflict in the rules entered for an access profile, the rule with the highest priority (lowest **access_id**) will take precedence.

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

Due to a chipset limitation, the Switch supports a maximum of 3 CPU access profiles. The rules used to define the access profiles are limited to a total of 5 rules for each entry.

CPU Filtering may be universally enabled or disabled. Setting up CPU Interface. To configure CPU Interface Filtering, see the descriptions below for **create cpu access_profile** and **config cpu access_profile**. To enable CPU Interface Filtering, see **config cpu_interface_filtering**.

Command	Parameters
create cpu access_profile	profile_id <value 1-3> [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | 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 {user_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]
delete cpu access_profile	profile_id <value 1-3>
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 <value0-7> | 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] | delete access_id <value 1-5>]
enable cpu_interface_filtering	
disable cpu_interface_filtering	
show cpu_access_profile	profile_id <value 1-3>

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

create cpu access_profile

Purpose	Used to create an access profile specifically for **CPU Interface Filtering** on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.
Syntax	**create cpu access_profile profile_id <value 1-3> [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | 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 {user_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]**
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	*profile_id* <*value 1-3*> – Specifies an index number that will identify the access profile being created with this command.
	
	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 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.

create cpu access_profile

- *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* – Specifies that the Switch will examine each frame's Protocol ID field.
  - *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.

Restrictions Only administrator-level users can issue this command.

Example usage:

To create a CPU access profile:

```
DES-3026:4#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-3026:4#
```

delete cpu access_profile

Purpose	Used to delete a previously created access profile or 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 5 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu**

delete cpu access_profile	
	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-3026:4#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3026:4#
```

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 <value0-7> | 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] | 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. 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.

config cpu access_profile

- *destination_mac <macaddr>* – Specifies that the access profile will apply to 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.

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.
  - *type <value 0-255>* – Specifies that the access profile will apply to this ICMP type value.
  - *code <value 0-255>* – Specifies that the access profile will apply to this ICMP code.
- *igmp* – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.
  - *type <value 0-255>* – Specifies that the access profile will apply to packets that have this IGMP type value.
- *tcp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.
  - *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.
  - *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.

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 t he 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.

config cpu access_profile

	• *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. *port <portlist>* - The access profile for the CPU may be defined for each port on the Switch. *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. *delete access_id <value 1-65535>* - Use this to remove a previously created access rule in a profile ID.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure a CPU access list entry:

```
DES-3026:4#config cpu access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 deny
Command: config cpu access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 deny

Success.

DES-3026:4#
```

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-3026:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3026:4#
```

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.

disable cpu_interface_filtering	
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable RMON:

```
DES-3026:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-3026:4#
```

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, and the current running state of the CPU filter.
Parameters	*profile_id <value 1-3>*- The user may select a profile to view the parameters currently set for this CPU access profile entry, based on a previously configured CPU access profile entry. Entering no parameter will display all information currently set for the CPU access profile function of the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To show the CPU filtering state on the Switch:

```
DES-3026:4#show cpu_access_profile
Command: show cpu_access_profile

CPU Interface Filtering State: Disabled

Access Profile Table

Access Profile ID: 1
Type   : Ethernet Frame Filter
Masks : VLAN
------------------------

Ports  : 2
ID Mode
---  ---------  --------------------
1   Permit   Default

Total Entries: 1

DES-3026:4#
```

24

PORT SECURITY COMMANDS

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

Command	Parameters
config port_security ports	[<portlist> | all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-10> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}
show port_security	{ports <portlist>}
delete port_security_entry vlan_name	<vlan_name 32> mac_address <macaddr> port <port>
clear port_security_entry port	<portlist>
enable port_security trap_log	
disable port_security trap_log	

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

NOTE: The uplink module ports (DES-3010F/FL/G ports 9-10, DES-3018 ports 17-18, DES-3026 ports 25-26) do not support the port security function.

config port_security ports

Purpose	Used to configure port security settings.
Syntax	**config port_security ports [<portlist> | all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-10> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <*portlist*> are effected.
Parameters	*ports <portlist>* – Specifies a port or range of ports to be configured for port security. *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 0-10>* - Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports. *lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]* – Indicates the method of locking addresses. The user has three choices: ▪ *Permanent* – The locked addresses will not age out after the aging timer expires. ▪ *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. ▪ *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-3026:4#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-3026:4#
```

show port_security

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

Example usage:

To display the port security configuration:

```
DES-3026:4#show port_security ports 1-8
Command: show port_security ports 1-8

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

DES-3026:4#
```

delete port_security_entry_vlan_name

Purpose	Used to delete an entry from the Switch's port security settings.
Syntax	**delete port_security_entry vlan_name <vlan_name 32> mac_address <macaddr> port <port>**
Description	This command is used to remove an entry from the port security entries learned by the Switch and entered into the forwarding database.
Parameters	*vlan_name* <*vlan_name 32*> - Enter the corresponding VLAN of the entry to delete. *mac_address* <*macaddr*> - Enter the corresponding MAC address of the entry to delete. *port* <*port*> - Enter the corresponding port of the entry to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an entry from the port security list:

```
DES-3026:4#delete port_security_entry vlan_name default
mac_address 00-0C-6E-73-2B-C9 port 1
Command: delete port_security_entry vlan_name default
mac_address 00-0C-6E-73-2B-C9 port 1

Success

DES-3026:4#
```

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 <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	*<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-3026:4#clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DES-3026:4#
```

enable port_security trap_log

Purpose	Used to enable the trap log function for port security.
Syntax	**enable port_security trap_log**
Description	This command is used to send trap messages to the Switch's log when a new MAC address violates the pre-defined port security configuration. This information will include the MAC address of the undefined device along with the port being infringed upon.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable the port security log trap function:

```
DES-3026:4# enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3026:4#
```

disable port_security trap_log

Purpose	Used to disable the trap log function for port security.
Syntax	**disable port_security trap_log**
Description	This command is used to disable sending trap messages to the Switch's log when a new MAC address violates the pre-defined port security configuration. This information will include the MAC address of the undefined device along with the port being infringed upon.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

```
DES-3026:4#disable port_security trap_log
Command: disable port_security trap_log

Success.

DES-3026:4#
```

25

802.1X COMMANDS

The DES-3000 switch series implements the server-side of the IEEE 802.1x Port-based and MAC-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames.

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

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

NOTE: The uplink module ports (DES-3010F/FL/G ports 9-10, DES-3018 ports 17-18, DES-3026 ports 25-26) do not support the 802.1X function.

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 Port-based or MAC-based Network Access control server application on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable 802.1x switch wide:

```
DES-3026:4#enable 802.1x
Command: enable 802.1x

Success.

DES-3026:4#
```

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 Port-based or MAC-based Network Access control server 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-3026:4#disable 802.1x
Command: disable 802.1x

Success.

DES-3026:4#
```

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 authentication mode command is used to enable either the port-based or MAC-based 802.1x authentication feature on the Switch.
Parameters	*[port_based | mac_based ports]* – The Switch may 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-3026:4#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DES-3026:4#
```

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 <portlist>}**
Description	The **show 802.1x auth_state** is used to display the current 802.1x authentication state of the specified ports of the Port-based or MAC-based Network Access Control server application on the Switch. The following details what is displayed: Port number – Shows the physical port number on the Switch, in port-based mode only. MAC Address – Displays the MAC address of the Switch in MAC-based mode only. Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE. Backend State: Request / Response / Fail / Idle / Initialize / 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.
Parameters	*ports <portlist>* – Specifies a port or range of ports to be viewed.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x authentication states (stacking disabled) for Port-based 802.1x:

```
DES-3026:4#show 802.1x auth_state ports 1-5
Command: show 802.1x auth_state ports 1-5

Port   Auth PAE State  Backend State  Port Status
------ --------------  -------------  ------------
1      ForceAuth       Success        Authorized
2      ForceAuth       Success        Authorized
3      ForceAuth       Success        Authorized
4      ForceAuth       Success        Authorized
5      ForceAuth       Success        Authorized

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

Example usage:

To display the 802.1x authentication states (stacking disabled) for MAC-based 802.1x:

```
DES-3026:4#show 802.1x auth_state
Command: show 802.1x auth_state

Port number : 1
Index  MAC Address        Auth PAE State      Backend State       Port Status
------ ------------------ ------------------- ------------------- ----------------
1      00-08-02-4E-DA-FA  Authenticated       Idle                Authorized
2
3
4
5
6
7
8

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

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 <portlist>}**
Description	The show 802.1x command is used to display the current configuration of the 802.1x Port-based Network Access Control server application on the Switch. The following details what is displayed: 802.1x Enabled/Disabled – Shows the current status of 802.1x functions on the Switch. Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the Switch and a RADIUS server. 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 four 802.1x capabilities that can be set on the Switch: Authenticator, Supplicant, Authenticator and Supplicant, and None. 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 can not access the network. PAE State: Initialize/Disconnected/Connecting/ Authenticating/Authenticated/Held

show 802.1x auth_configuration

	/ForceAuth/ForceUnauth – Shows the current state of the Authenticator PAE. Backend State: Request/Response/Fail/Idle/Initialize – Shows the current state of the Backend Authenticator. 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 – Shows the time interval between authentication failure and the start of a new authentication attempt. TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets. 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.
Parameters	*ports <portlist>* – Specifies a port or range of ports to be viewed.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x configurations:

```
DES-3026:4#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
```

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 four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, 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-3026:4#config 802.1x capability ports 1–10 authenticator
Command: config 802.1x capability ports 1–10 authenticator

Success.

DES-3026:4#
```

config 802.1x auth_parameter ports

Purpose	Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	**config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]**
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	*<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. ▪ *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.

config 802.1x auth_parameter ports	
	▪ *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-3026:4#config 802.1x auth_parameter ports 1 – 20 direction both
Command: config 802.1x auth_parameter ports 1 – 20 direction both

Success.

DES-3026:4#
```

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 you to configure the authentication protocol.
Parameters	*[local | radius_eap]* – Specify the type of authentication protocol desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the authentication protocol on the Switch:

```
DES-3026:4# config 802.1x auth_protocol local
Command: config 802.1x auth_protocol local

Success.

DES-3026:4#
```

config 802.1x init	
Purpose	Used to initialize the 802.1x function on a range of ports.
Syntax	**config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]**
Description	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 ports* – This instructs the Switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified. ▪ *<portlist>* – Specifies a port or range of ports to be initialized. ▪ *all* – Specifies all of the ports on the Switch to be initialized. *mac_based* - This instructs the Switch to initialize 802.1x functions based on the MAC address of a device on a specific port or range of ports. MAC address approved for initialization can then be specified. ▪ *ports <portlist>* – Specifies a port or range of ports. ▪ *all* – Specifies all of the ports on the Switch. *mac_address <macaddr>* - Specifies the MAC address of the client to be added.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To initialize the authentication state machine of some or all:

```
DES-3026:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-3026:4#
```

config 802.1x reauth	
Purpose	Used to configure the 802.1x re-authentication feature of the Switch.
Syntax	**config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]**
Description	The **config 802.1x reauth** command is used to re-authenticate a previously authenticated device based on a port number.
Parameters	*port_based* – This instructs the Switch to re-authorize 802.1x function based only on the port number. Ports approved for re-authorization can then be specified. ▪ *ports <portlist>* – Specifies a port or range of ports to be reauthorized. ▪ *all* – Specifies all of the ports on the Switch to be reauthorized. *mac-based* - This instructs the Switch to re-authorize 802.1x function based on a specific MAC address. Ports approved for re-authorization can then be specified. ▪ *ports <portlist>* – Specifies a port or range of ports. ▪ *all* – Specifies all ports on the Switch.

config 802.1x reauth	
	mac_address <macaddr> - Specifies the MAC address of the client to add.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-18:

```
DES-3026:4#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-3026:4#
```

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. *<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* – Returns all of the ports in the range to their default RADIUS 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 RADIUS server communication settings:

```
DES-3026:4#config radius add 1 10.48.74.121 key tomato default
Command: config radius add 1 10.48.74.121 key tomato default

Success.

DES-3026:4#
```

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 three groups of RADIUS server settings can be entered on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DES-3026:4#config radius delete 1
Command: config radius delete 1

Success.

DES-3026:4#
```

config radius	
Purpose	Used to configure the Switch's RADIUS settings.
Syntax	**config radius <server_index 1-3> {ipaddress <server_ip> | key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}**
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. *<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* – Returns all of the ports in the range to their default RADIUS 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 RADIUS settings:

```
DES-3026:4#config radius 1 10.48.74.121 key dlink default
Command: config radius 1 10.48.74.121 key dlink default

Success.

DES-3026:4#
```

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-3026:4#show radius
Command: show radius

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-3026:4#
```

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-3026:4#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-3026:4#
```

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 MAC-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-3026:4#show 802.1x user
Command: show 802.1x user

Index           User Name
--------------  --------------
1               Trinity

The Total Entry is : 1

DES-3026:4#
```

delete 802.1x user

Purpose	Used to delete an 802.1x user account on the Switch.
Syntax	**delete 802.1x user <username 15> {force_agree}**
Description	The **delete 802.1x user** command is used to delete the 802.1x Port-based or MAC-based Network Access control local users currently configured on the Switch.
Parameters	*<username 15>* – A username can be as many as 15 alphanumeric characters. *force_agree* – Entering this parameter will bypass the “Are you sure?” question and immediately delete the account.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete 802.1x users:

```
DES-3026:4#delete 802.1x user dtremblett
Command: delete 802.1x user dtremblett

Success.

DES-3026:4#
```

show radius 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-3026:4#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 radius 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-3026:4#show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses      0
radiusAuthClientIdentifier                  D-Link

radiusAuthServerEntry ==>
radiusAuthServerIndex    : 1

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

show auth_diagnostics

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

Example usage:

To display the current authentication diagnostics for port 16:

```
DES-3026:4#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 [<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 <portlist>* – Specifies a port or range of ports to be viewed. *all* – Specifies that all ports will be viewed.
Restrictions	None.

Example usage:

To display the current authentication session statistics for port 16:

```
DES-3026:4#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 <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 <portlist>* – Specifies a range of ports to be viewed.
Restrictions	None.

Example usage:

To display the current authentication statistics for port 1:

```
DES-3026:4#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 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 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 a 802.1x Guest VLAN for the Switch.

```
DES-3026:4#create 802.1x guest_vlan Trinity
Command: create 802.1x guest_vlan Trinity

Success.

DES-3026:4#
```

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-3026:4#config 802.1x guest_vlan ports 1-5 state enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DES-3026:4#
```

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 limited access rights on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

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

```
DES-3026:4#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-----------------------------------------------------------
Guest VLAN : Trinity
Enable Guest VLAN ports: 5-8

DES-3026:4#
```

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 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-3026:4#delete 802.1x guest_vlan Trinity
Command: delete 802.1x guest_vlan Trinity

Success.

DES-3026:4#
```

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_wday <start_weekday sun-sat>| s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e-wday <end_weekday sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]
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 the SNTP information will be taken from. ▪ *<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* – This is the interval between requests for updated SNTP information. ▪ *<int 30-99999>* – The polling interval ranges from 30 to 99,999 seconds. The default setting is 720 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-3026:4#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-3026:4#
```

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-3026:4#show sntp
Command: show sntp

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

DES-3026:4#
```

enable sntp	
Purpose	Enables 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-3026:4#enable sntp
Command: enable sntp

Success.

DES-3026:4#
```

disable sntp	
Purpose	Disables 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:

To stop SNTP support:

```
DES-3026:4#disable sntp
Command: disable sntp

Success.

DES-3026:4#
```

config time	
Purpose	Used to manually configure system time and date settings.
Syntax	**config time date <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-3026:4#config time 30062003 16:30:30
Command: config time 30062003 16:30:30

Success.

DES-3026:4#
```

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.

config time_zone	
Parameters	*operator* – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT. *hour* – Select the number hours offset from GMT (Greenwich Mean Time). *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-3026:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3026:4#
```

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_wday <start_weekday sun-sat>| s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e-wday <end_weekday sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]**
Description	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_wday* – Configure the day of the week in which DST begins. • <*start_weekday sun-sat*> - The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)

config dst	
	e_wday - Configure the day of the week in which DST ends. • <*end_weekday sun-sat*> - The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *s_mth* - Configure the month in which DST begins. • <*start_mth 1-12*> - The month to begin DST expressed as a number. *e_mth* - Configure the month in which DST ends. • <*end_mth 1-12*> - The month to end DST expressed as a number. *s_time* – Configure the time of day to begin DST. • <*start_time hh:mm*> - Time is expressed using a 24-hour clock, in hours and minutes. *e_time* - Configure the time of day to end DST. • <*end_time hh:mm*> - Time is expressed using a 24-hour clock, in hours and minutes. *s_date* - Configure the specific date (day of the month) to begin DST. • <*start_date 1-31*> - The start date is expressed numerically. *e_date* - Configure the specific date (day of the month) to begin DST. • <*end_date 1-31*> - The end date is expressed numerically. *offset [30 | 60 | 90 | 120]* - Indicates number of minutes to add or to subtract during the summertime. The possible offset times are 30, 60, 90, 120. The default value is 60.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DES-3026:4# config dst repeating s_week 2 s_wday tue s_mth 4
s_time 15:00 e_week 2 e_wday wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_wday tue s_mth 4 s_time
15:00 e_week 2 e_wday wed e_mth 10 e_time 15:30 offset 30

Success.

DES-3026:4#
```

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 settings:

```
DES-3026:4#show time
Command: show time

Current Time Source  : System Clock
Current Time         : 0 Days 01:09:49
Time Zone            : GMT -06:00
Daylight Saving Time : Disabled
Offset in minutes    : 60
   Repeating From    : Apr 1st Sun 00:00
               To    : Oct last Sun 00:00
   Annual      From  : 29 Apr 00:00
               To    : 12 Oct 00:00

DES-3026:4#
```

27

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

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-3026:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DES-3026:4#
```

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-3026:4#delete iproute default 10.53.13.254
Command: delete iproute default 10.53.13.254

Success.

DES-3026:4#
```

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* – IP address and netmask of the IP interface that is the destination of the route. The address and mask information may be specified by using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *static* - Use this parameter to display static iproute entries.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DES-3026:4#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-3026:4#
```

28

ARP COMMANDS

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

Command	Parameters
show arpentry	{ipif <ipif_name 12> | ipaddress <ipaddr> | static}
config arp_aging time	<value 0-65535>
clear arptable	

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

show arpentry	
Purpose	Used to display the ARP table.
Syntax	**show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static}**
Description	This command is used to display the current contents of the Switch's ARP table.
Parameters	*<ipif_name 12>* – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. *<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-3026:4#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          10.1.1.169      00-50-BA-70-E4-4E   Dynamic
System          10.1.1.254      00-01-30-FA-5F-00   Dynamic
System          10.9.68.1       00-A0-C9-A4-22-5B   Dynamic
System          10.9.68.4       00-80-C8-2E-C7-45   Dynamic
System          10.10.27.51     00-80-C8-48-DF-AB   Dynamic
System          10.11.22.145    00-80-C8-93-05-6B   Dynamic
System          10.11.94.10     00-10-83-F9-37-6E   Dynamic
System          10.14.82.24     00-50-BA-90-37-10   Dynamic
System          10.15.1.60      00-80-C8-17-42-55   Dynamic
System          10.17.42.153    00-80-C8-4D-4E-0A   Dynamic
System          10.19.72.100    00-50-BA-38-7D-5E   Dynamic
System          10.21.32.203    00-80-C8-40-C1-06   Dynamic
System          10.40.44.60     00-50-BA-6B-2A-1E   Dynamic
System          10.42.73.221    00-01-02-03-04-00   Dynamic
System          10.44.67.1      00-50-BA-DA-02-51   Dynamic
System          10.47.65.25     00-50-BA-DA-03-2B   Dynamic
System          10.50.8.7       00-E0-18-45-C7-28   Dynamic
```

```
System          10.90.90.90      00-01-02-03-04-00      Local
System          10.255.255.255   FF-FF-FF-FF-FF-FF      Local/Broadcast

Total Entries = 20

DES-3026:4#
```

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-3026:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3026:4#
```

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-3026:4#clear arptable
Command: clear arptable

Success.

DES-3026:4#
```

29

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 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 up to 33 switches (numbered 0-32), including the Commander Switch (numbered 0).
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The Switch may take on three different roles:

Commander Switch (CS) – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:

- It has an IP Address.
- It is not a commander switch or member switch of another Single IP group.
- It is connected to the member switches through its management VLAN.

Member Switch (MS) – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:

- It is not a CS or MS of another IP group.
- It is connected to the CS through the CS management VLAN.

Candidate Switch (CaS) – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group 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 a Candidate 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 switches may join the group by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CaS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

To join an SIM group, first enable the Switch for SIM using the **enable sim** command. Once enabled the switch is ready to join an SIM group yet to be a part of that group, the commander switch must be configured to accept the DES-3000 switch as a member switch. For more information on adding the DES-3000 switch as a member of an SIM group, please see the commander switch's user guide or command line interface reference manual.

The D-Link Single IP Management commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable sim	
disable sim	
show sim	{[candidates {<candidate_id 1-100>} | members {<member_id 1-32>} | group {commander_mac <macaddr>} | neighbor]}
reconfig	[member_id <value 1-32> | exit]
config sim_group	[add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]
config sim	[[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>]
download sim_ms	[firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}
upload sim_ms configuration	[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-3026:4#enable sim
Command: enable sim

Success.

DES-3026:4#
```

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-3026:4#disable sim
Command: disable sim

Success.

DES-3026:4#
```

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. 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 candidate 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 of a commander device, identified by its MAC address. *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:

show sim	
	• 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	Only administrator-level users can issue this command.

Example usage:

To show the SIM information in detail:

```
DES-3026:4#show sim
Command: show sim

SIM Version          : VER-1.61
Firmware Version     : Build 4.00.011
Device Name          :
MAC Address          : 00-35-26-11-11-00
Capabilities         : L3
Platform             : DES-3026 L2 Switch
SIM State            : Enabled
Role State           : Commander
Discovery Interval   : 30 sec
Hold Time            : 100 sec

DES-3026:4#
```

To show the candidate information in summary, if the candidate ID is specified:

```
DES-3026:4#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-3018 L2 Switch       40     4.00.011  The Man
2    00-55-55-00-55-00  DES-3026 L2 Switch       140    4.00.011  default master

Total Entries: 2

DES-3026:4#
```

To show the member information in summary, if the member ID is specified:

```
DES-3026:4#show sim members
Command: show sim members

ID   MAC Address        Platform /              Hold   Firmware   Device Name
                        Capability              Time   Version
---  -----------------  ----------------------  ----   ---------  ----------------
1    00-01-04-03-04-00  DES-3018 L2 Switch       40     4.00.011  The Man
2    00-55-35-00-55-00  DES-3026 L2 Switch       140    4.00.011  default master

Total Entries: 2

DES-3026:4#
```

To show other groups information in summary, if group is specified:

```
DES-3026:4#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-3018 L2 Switch      40     4.00.011   Trinity

SIM Group Name : default

ID  MAC Address        Platform /              Hold   Firmware   Device Name
                       Capability              Time   Version
--- -----------------  ----------------------  -----  ---------  ----------------
 2  00-55-55-00-55-00  DES-3018 L2 Switch      140    4.00.011    Enrico

SIM Group Name : SIM2

ID   MAC Address        Platform /              Hold    Firmware   Device Name
                        Capability              Time    Version
---  -----------------  ----------------------  ------  ---------  ----------------
*1   00-01-02-03-04-00  DES-3018 L2 Switch      40      4.00.011   Neo
 2   00-55-55-00-55-00

'*' means commander switch.

DES-3026:4#
```

Example usage:

To view SIM neighbors:

```
DES-3026:4#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-3026:4#
```

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-3026:4#reconfig member_id 2
Command: reconfig member_id 2


DES-3026:4#
```

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 it ID number.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add a member:

```
DES-3026:4#config sim_group add 2
Command: config sim_group add 2

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

Success.

DES-3026:4#
```

To delete a member:

```
DES-3026:4#config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK...

Success.

DES-3026:4#
```

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 <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 for the following parameters: *group_name <groupname 64>* - Used to update the name of the group. Enter an alphanumeric string of up to 64 characters to rename the SIM group. *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 commander switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the discovery protocol interval from 30 to 90 seconds. *hold time <sec 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. *candidate* – Used to change the role of a commander switch to a candidate switch. *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 commander switch 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 <sec 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-3026:4#config sim commander dp_interval 30
Command: config sim commander dp_interval 30

Success.

DES-3026:4#
```

To change the hold time of the discovery protocol:

```
DES-3026:4#config sim commander hold_time 120
Command: config sim commander hold_time 120

Success.

DES-3026:4#
```

To transfer the commander switch to be a candidate:

```
DES-3026:4#config sim candidate
Command: config sim candidate

Success.

DES-3026:4#
```

To transfer the Switch to be a commander:

```
DES-3026:4#config sim commander
Command: config sim commander

Success.

DES-3026:4#
```

To update the name of a group:

```
DES-3026:4#config sim commander group_name Trinity
Command: config sim commander group_name Trinity

Success.

DES-3026:4#
```

download sim_ms

Purpose	Used to download firmware or configuration file to an indicated device.
Syntax	**download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}**
Description	This command will download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	*firmware_from_tftp* – Specify this parameter to download firmware to members of a SIM group. *configuration_from_tftp* - 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 to download firmware or switch configuration files. The user may specify a member or members by adding one of the following: • <*mslist 1-32*> - 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-3026:4#download sim_ms firmware 10.53.13.94 c:/des3000.had members all
Command: download sim_ms firmware 10.53.13.94 c:/des3000.had members all

This device is updating firmware.  Please wait...

Download Status :

ID   MAC Address       Result
---  ----------------  ----------------
1    00-01-02-03-04-00 Success
2    00-07-06-05-04-03 Success
3    00-07-06-05-04-03 Success

DES-3026:4#
```

To download configuration files:

```
DES-3026:4#download sim_ms configuration 10.53.13.94 c:/dgssri.txt members all
Command: download sim_ms configuration 10.53.13.94 c:/dgssri.txt members all

This device is updating configuration.  Please wait...

Download Status :

ID   MAC Address       Result
---  ----------------  ----------------
1    00-01-02-03-04-00 Success
2    00-07-06-05-04-03 Success
3    00-07-06-05-04-03 Success

DES-3026:4#
```

upload sim_ms	
Purpose	Used 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	*configuration_to_tftp* - Specify this parameter to upload a switch configuration file to a TFTP server. *log_to_tftp* - Specify this parameter to upload a switch log file to a TFTP server. <*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. *members* – Enter this parameter to specify the members from which to upload a log file or switch configuration file. 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 from which log or configuration files will be uploaded . • *all* – Add this parameter to specify all members of the SIM group from which log or configuration files will be uploaded
Restrictions	Only administrator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DES-3026:4#upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1
Command: upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1

Success.

DES-3026:4#
```

30

COMMAND HISTORY LIST

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

Command	Parameters
?	{<command>}
show command_history	
dir	
config command_history	<value 1-40>

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-3026:4#?
Command: ?
..
?
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 guest_vlan ports
config 802.1x init
config 802.1x reauth
config account
config address_binding ip_mac ipaddress
config address_binding ip_mac ports
config arp_aging time
config bandwidth_control
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

Example usage:

To display the parameters for a specific command:

```
DES-3026:4#? config igmp_snooping
Command: config igmp_snooping

Command: config igmp_snooping
Usage: [vlan_name <vlan_name 32> | all] {host_timeout <sec 1-16711450> |
router_timeout <sec 1-16711450> | leave_timer <sec 1-16711450> | state
[enabled | disabled | fast_leave [enabled | disabled]}
Description: Used to configure IGMP snooping on the switch.
config igmp_snooping querier

DES-3026:4#
```

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-3026:4#show command_history
Command: show command_history

?
? show
show vlan
config router_ports vlan2 add 1:1-1:10
config router_ports vlan2 add
config router_ports vlan2
config router_ports
show vlan
create vlan vlan2 tag 3
create vlan vlan2 tag 2
show router_ports
show router ports
login

DES-3026:4#
```

dir

Purpose	Used to display all commands.
Syntax	**dir**
Description	This command will display all commands.
Parameters	None.
Restrictions	None.

Example usage

To display all of the commands:

```
DES-3026:4#dir
Command: 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 guest_vlan ports
config 802.1x init
config 802.1x reauth
config account
config address_binding ip_mac ipaddress
config address_binding ip_mac ports
config arp_aging time
config bandwidth_control
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-3026:4#config command_history 20
Command: config command_history 20

Success.

DES-3026:4#
```

A

TECHNICAL SPECIFICATIONS

Physical and Environmental	
AC input	100 –240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	DES-3010FL – 14.8W DES-3010F – 15W DES-3010G – 14.8W DES-3018 – 15.2W DES-3026 – 17W
Operating Temperature:	0 to 40 degrees Celsius
Storage Temperature:	-40 to 70 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	DES-3010F/G - 280 mm x 180 mm x 44 mm (1U), 11 inch rack-mount width DES-3018/3026 - 441 mm x 207mm x 44 mm (1U), 19 inch rack-mount width
Weight:	DES-3010F//FL/G – 1.5kg DES-3018 and DES-3026 - 2.1 kg
EMI:	FCC Class A, CE Class A, C-Tick Class A,VCCI Class A
Safety:	CSA International

General	
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX Gigabit Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 d/w Spanning Tree IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation
Protocols:	CSMA/CD
Data Transfer Rates	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
Network Cables:	
10BASE-T	2-pair UTP Cat. 3,4,5 (100 m) EIA/TIA- 568 100-ohm STP (100 m)
100BASE-TX	2-pair UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)
Number of Ports	DES-3010F - 8 x 10/100 Mbps NWay ports, 1 x 1000BASE-T Gigabit Port, 1 x 100BASE-FX (MM) Fiber Optic Port DES-3010FL - 8 x 10/100 Mbps NWay ports, 1 x 1000BASE-T Gigabit Port, 1 x 100BASE-FX (SM) Fiber Optic Port DES-3010G - 8 x 10/100 Mbps NWay ports, 1 x 1000BASE-T Gigabit Port, 1 x SFP Fiber Optic Port DES-3018 - 16 x 10/100 Mbps NWay ports + 2 Optional Module Slots DES-3018 - 24 x 10/100 Mbps NWay ports + 2 Optional Module Slots DEM-301T (Optional Module) – 1 x 1000BASE-T Gigabit Port DEM-201F (Optional Module) – 1 x 100BASE-FX (MM) Port DEM-201FL(Optional Module) – 1 x 100BASE-FX (SM) Port DEM-301G (Optional Module) – 1 SFP Gigabit Port

Performance	
Transmission Method	Store-and-forward
RAM Buffer	32M Bytes per device
Filtering Address Table:	8K MAC address per device
Packet Filtering / Forwarding Rate:	14,880 pps per 10Mbps 148,809 pps per 100Mbps 1,488,100 pps per 1000Mbps
MAC Address Learning	Automatic update.