



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

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

Command Line Interface Reference Manual

First Edition (May 2005)

651ES3026015

Printed In Taiwan



RECYCLABLE

Table of Contents

Introduction	1
Using the Console CLI	4
Command Syntax	9
Basic Switch Commands	11
Switch Port Commands	23
Network Management (SNMP) Commands	26
Download/Upload Commands	47
Network Monitoring Commands	49
Spanning Tree Commands	61
Forwarding Database Commands	67
Broadcast Storm Control Commands	73
QoS Commands	75
Traffic Segmentation Commands	84
Port Mirroring Commands	86
VLAN Commands	89
Link Aggregation Commands	92
Basic IP Commands	97
IGMP Snooping Commands	99
Port Security Commands	105
802.1X Commands	108
Time and SNTP Commands	124
Routing Table Commands	130
ARP Commands	132
D-Link Single IP Management Commands	135
Command History List	140
Technical Specifications	143

INTRODUCTION

This document is a reference guide for all DES-3010F/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-3010G/DES-3018/DES-3026 switches contain the same information and possess 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.

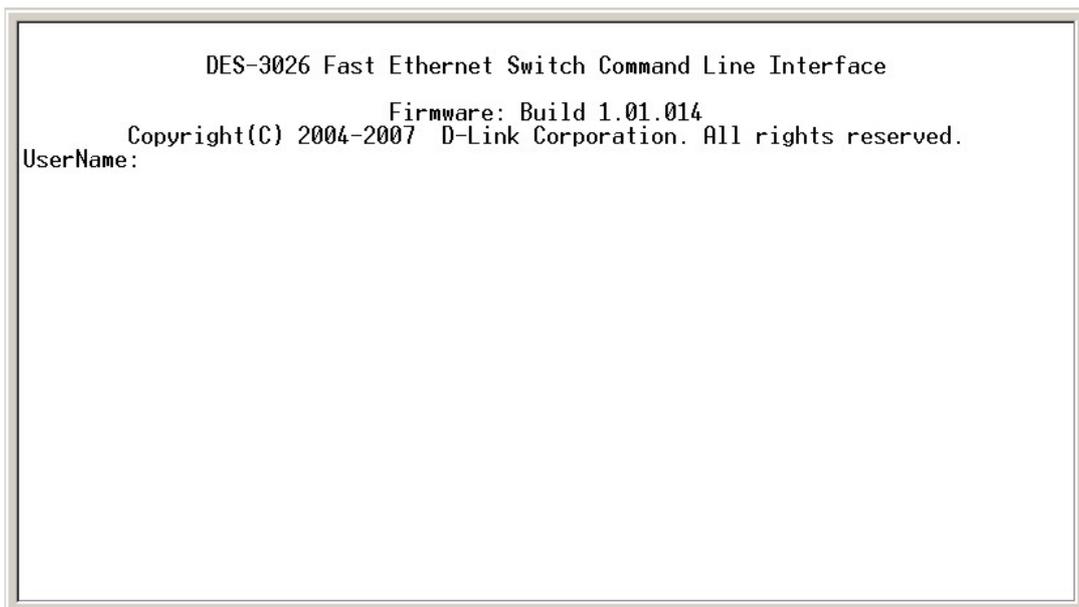
Accessing the Switch via the Serial Port

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.



```
DES-3026 Fast Ethernet Switch Command Line Interface
                          Firmware: Build 1.01.014
Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
UserName:
```

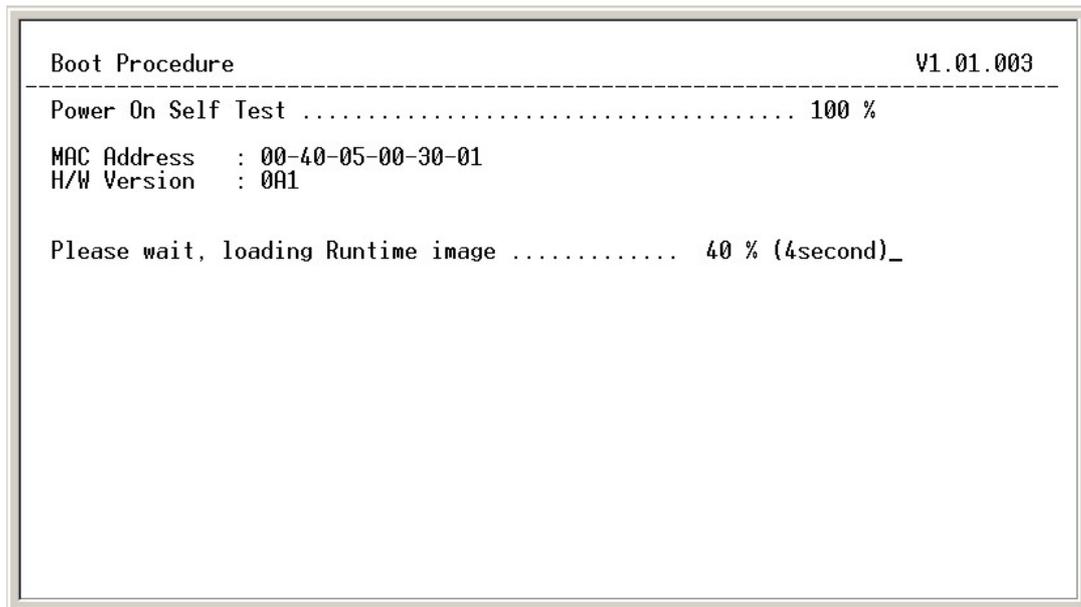
Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-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. You can change the default Switch IP address to meet the specification of your networking address scheme.

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



```
Boot ProcedureV1.01.003
-----
Power On Self Test ..... 100 %
MAC Address   : 00-40-05-00-30-01
H/W Version   : 0A1

Please wait, loading Runtime image ..... 40 % (4second)_
```

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.

```
DES-3026 Fast Ethernet Switch Command Line Interface
                          Firmware: Build 1.01.014
Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
UserName:
Password:
DES-3026:4#config ipif System ipaddress 10.53.13.111/255.0.0.0
Command: config ipif System ipaddress 10.53.13.111/8

Success.
DES-3026:4#
```

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.53.13.111 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.

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**
- **9,600 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-3026 Fast Ethernet Switch Command Line Interface
                          Firmware: Build 1.01.014
Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
UserName:
Password:
DES-3026:4#
```

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.

```
?
clear
clear arptable
clear counters
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config account
config arp_aging time
config bandwidth_control
config command_history
config dst
config fdb_aging_time
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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.

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

Next possible completions:
 802.1p 802.1x account arprentry auth_diagnostics auth_session_statistics
auth_statistics bandwidth_control command_history config error fdb
igmp_snooping ipif iproute lACP_port link_aggregation log mirror
multicast_fdb packet port_security ports radius router_ports scheduling
scheduling_mechanism serial_port session sim snmp snmp stp switch
syslog time traffic traffic_segmentation trusted_host utilization vlan

DES-3026:4#
```

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.

```
DES-3026:4#config account
Command: config account

Next possible completions:
 <username>

DES-3026:4#config account
Command: config account

Next possible completions:
 <username>

DES-3026:4#
```

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

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

```
DES-3026:4#the
Available commands:
  .. ? clear config create delete dir disable download enable login
      logout ping reboot reset save show upload
DES-3026:4#
```

Figure 2-5. The Next Available Commands Prompt

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

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

```
DES-3026:4#show
Command: show
Next possible completions:
  802.1p 802.1x account arprentry auth_diagnostics auth_session_statistics
  auth_statistics bandwidth_control command_history config error fdb
  igmp_snooping ipif iproute lacp_port link_aggregation log mirror
  multicast_fdb packet port_security ports radius router_ports scheduling
  scheduling_mechanism serial_port session sim snmp sntp stp switch
  syslog time traffic traffic_segmentation trusted_host utilization vlan
DES-3026:4#
```

Figure 2-6. Next possible completions: show command

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

COMMAND SYNTAX

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual. The online help contained in the CLI and available through the console interface uses the same syntax.



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

<angle brackets>

Purpose	Encloses a variable or value that must be specified.
Syntax	config ipif <ipif_name 12> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable]}] bootp dhcp
Description	In the above syntax example, you must supply an IP interface name in the <ipif_name> space, a VLAN name in the <vlan_name 32> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	config ipif System ipaddress 10.24.22.5/255.0.0.0 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]
Description	In the above syntax example, you must specify either an admin or a user level account to be created. Do not type the square brackets.
Example Command	create account admin

| 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, you must specify either a VLAN , or a MAC address by which to show multicast FDB entries. Do not type the vertical bar.
Example Command	show snmp community

{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.

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>
show account	
show session	
show switch	
show config	[dram flash]
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]}}
login	
logout	
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}

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 consist of a username of 1 to 15 characters and a password of 0 to 15 characters. Up to 8 user accounts can be created.
Parameters	<i>admin</i> <username> <i>user</i> <username>
Restrictions	Only Administrator-level users can issue this command.

create account

Username can be between 1 and 15 characters.

Password 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#
```

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	None.

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

Total Entries: 1

DES-3026:4#
```

delete account

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

Example usage:

To delete the user account “System”:

```
DES-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.
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
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 1.01.003
Firmware Version  : Build 1.01.014
Hardware Version  : 0A1
System Name       : DES-3026_#3
System Location   : 7th_flr_east_cabinet
System Contact    : Julius_Erving_212-555-6666
Spanning Tree     : Disabled
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 [dram flash]
Description	This command displays a list of configuration commands entered into the Switch.
Parameters	<p><i>dram</i> – Entering this parameter will display configurations saved to the DRAM memory in the Switch.</p> <p><i>flash</i> - Entering this parameter will display configurations saved to the flash memory of the switch.</p>
Restrictions	None.

Example usage:

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

```
DES-3026:4# show config dram
```

```
Command: show config dram
```

```
# BASIC
```

```
config serial_port baud_rate 115200 auto_logout never
```

```
enable telnet 23
```

```
enable web 80
```

```
enable clipaging
```

```
# STORM
```

```
config traffic control 1-16 broadcast disable multicast disable dif disable  
threshold 128
```

```
config traffic control 1-16 broadcast disable multicast disable dif 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	<p><i>baud_rate [9600 19200 38400 115200]</i> – The serial bit rate that will be used to communicate with the management host.</p> <p><i>auto_logout</i> - 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.</p> <ul style="list-style-type: none"> ▪ <i>never</i> – No time limit on the length of time the console can be open with no user input. ▪ <i>2_minutes</i> – The console will log out the current user if there is no user input for 2 minutes. ▪ <i>5_minutes</i> – The console will log out the current user if there is no user input for 5 minutes. ▪ <i>10_minutes</i> – The console will log out the current user if there is no user input for 10 minutes. ▪ <i>15_minutes</i> – 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

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>

enable telnet

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	<i><tcp_port_number 1-65535></i> – 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. The user can specify the TCP port number the Switch will use to listen for Telnet requests.
Parameters	<i><tcp_port_number 1-65535></i> – The TCP port number. TCP ports

enable web

	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
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	None.
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
Description	This command is used to restart the Switch.
Parameters	None.
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]}
Description	This command is used to restore the Switch's configuration to the default settings assigned from the factory.
Parameters	<p><i>config</i> – If the keyword 'config' is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, and the Switch history log. The Switch will not save or reboot.</p> <p><i>system</i> – If the keyword 'system' is specified all of the factory default settings are restored on the Switch. The Switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base.</p> <p>If no parameter is specified, the Switch's current IP address, user accounts, and the Switch history log are not changed. All other parameters are restored to the factory default settings. The Switch will not save or reboot.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3026:4#reset config
Command: reset config

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	<p><i><ipaddr></i> - Specifies the IP address of the host.</p> <p><i>times <value 1-255></i> - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 0.</p> <p><i>timeout <sec 1-99></i> - Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.</p> <p>Pinging an IP address without the <i>times</i> parameter will ping the target device an infinite amount of times.</p>
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#
```

SWITCH PORT COMMANDS

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

Command	Parameters
config ports	[<portlist> all] {speed [auto 10_half 10_full 100_half 100_full 1000_full {master slave}] flow_control [enable disable] state [enable disable] description [<desc 0-32> clear]}
show ports	{<portlist>} {description}

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 0-32> clear]}
Description	This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.
Parameters	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Configure all ports on the Switch.</p> <p><i>speed</i> – Allows the user to set the speed of a port or range of ports, with the addition of one of the following:</p> <ul style="list-style-type: none"> ▪ <i>auto</i> – Enables auto-negotiation for the specified range of ports. ▪ [<i>10</i> <i>100</i> <i>1000</i>] – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 and cannot be set to slower speeds. ▪ [<i>half</i> <i>full</i>] – Configures the specified range of ports as either full- or half-duplex. <p>[<i>master</i> <i>slave</i>] – The <i>master</i> and <i>slave</i> parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The <i>master</i> setting will allow the port to advertise capabilities related to duplex, speed and physical layer type. The <i>master</i> 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 <i>master</i> physical layer by a local source. The <i>slave</i> setting uses loop timing, where the timing comes from a data stream received from the <i>master</i>. If one connection is set for <i>1000 master</i>, the other side of the connection must be set for <i>1000 slave</i>. Any other configuration will result in a link down status for both ports.</p> <p><i>flow_control</i> [enable disable] – Enable or disable flow control for the specified ports.</p> <p><i>state</i> [enable disable] – Enables or disables the specified range of ports.</p>

config ports

description <desc 32> - Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.

clear – 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, learning 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}
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.
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 State	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address 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 State	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
-----	-----	-----	-----	-----
1	Enabled	Auto/Enabled	Link Down	Enabled

Description: Accounting

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

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 – NoAuthNoPriv
v3	MD5 or SHA	Authentication is based on the HMAC-MD5 or HMAC-SHA algorithms – AuthNoPriv
v3	MD5 DES or SHA DES	Authentication is based on the HMAC-MD5 or HMAC-SHA algorithms – AuthPriv. DES 32-bit encryption is added based on the CBC-DES (DES-32) standard

Command	Parameters
create snmp user	<SNMPname 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	<SNMPname 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included excluded]
delete snmp view	<view_name 32> [all oid]
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> view <view_name 32> [read_only read_write]
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID>
show snmp engineID	
create snmp group	<groupname 32> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] read view <view name 32> write view

Command	Parameters
	<view_name 32> notify_view <view_name 32>}
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	<ipaddr> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	{<ipaddr>}
enable rmon	
disable rmon	
create trusted_host	<ipaddr>
delete trusted_host	<ipaddr>
show trusted_host	<ipaddr>
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 <SNMPname 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	<p><SNMPname 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.</p> <p><groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be</p>

create snmp user

associated with.

encrypted – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose:

- *by_password* – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the *auth_password* below. This method is recommended.
- *by_key* – Requires the SNMP user to enter an encryption key for authentication and privacy. The key is defined by specifying the key in hex form below. This method is not recommended.

auth - The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are:

- *md5* – Specifies that the HMAC-MD5-96 authentication level will be used. *md5* may be utilized by entering one of the following:
 - *<auth_password 8-16>* - An alphanumeric string of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host.
 - *<auth_key 32-32>* - Enter an alphanumeric string of exactly 32 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host.
- *sha* – Specifies that the HMAC-SHA-96 authentication level will be used.
 - *<auth_password 8-20>* - An alphanumeric string of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.
 - *<auth_key 40-40>* - An alphanumeric string of exactly 40 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host.

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

- *des* – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using:
 - *<priv_password 8-16>* - An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.
 - *<priv_key 32-32>* - 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.

create snmp user

	<i>none</i> – 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 <SNMPname 32>
Description	The delete snmp user command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	<SNMPname 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.
Parameters	<p><i><view_name 32></i> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created.</p> <p><i><oid></i> – The object ID that identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.</p> <p><i>included</i> – Include this object in the list of objects that an SNMP manager can access.</p> <p><i>excluded</i> – Exclude this object from the list of objects that an SNMP manager can access.</p>
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	<p><view_name 32> – An alphanumeric string of up to 32 characters that identifies the SNMP view to be deleted.</p> <p><i>all</i> – Specifies that all of the SNMP views on the Switch will be deleted.</p> <p><oid> – The object ID that identifies an object tree (MIB tree) that will be deleted from the Switch.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DES-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 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	<p>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:</p> <ul style="list-style-type: none"> 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	<p><i><community_string 32></i> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.</p> <p><i><view_name 32></i> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.</p> <p><i>read_only</i> – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch.</p> <p><i>read_write</i> – Specifies that SNMP community members using the community string created with this command can read from and write</p>

create snmp community

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

Example usage:

To display the currently entered SNMP community strings:

```
DES-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>
Description	The config snmp engineID command configures a name for the SNMP engine on the Switch.
Parameters	<i><snmp_engineID></i> – An alphanumeric string that will be used to identify the SNMP engine on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-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	<p><i><groupname 32></i> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p><i>v1</i> – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p><i>v2c</i> – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>v3</i> – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <ul style="list-style-type: none"> ▪ Message integrity – Ensures that packets have not been tampered with during transit. ▪ Authentication – Determines if an SNMP message is from a valid source. ▪ Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source. <p><i>noauth_nopriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_priv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.</p>

create snmp group

read_view – Specifies that the SNMP group being created can 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 the new SNMP user will be associated with.

Restrictions Only administrator-level users can issue this command.

Example usage:

To delete the SNMP group named “sg1”.

```
DES-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	<p><i><ipaddr></i> – The IP address of the remote management station that will serve as the SNMP host for the Switch.</p> <p><i>v1</i> – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p><i>v2c</i> – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>v3</i> – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <ul style="list-style-type: none"> ▪ Message integrity – ensures that packets have not been tampered with during transit. ▪ Authentication – determines if an SNMP message is from a valid source. ▪ Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source. <p><i>noauth_nopriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_priv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.</p> <p><i><auth_sting 32></i> – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-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>
Description	The create trusted_host command creates the trusted host. The Switch allows you to specify up to four IP addresses that are allowed to manage the Switch via in-band SNMP or TELNET based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.
Parameters	<ipaddr> – The IP address of the trusted host to be created.
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#
```

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 {<ipaddr>}
Description	This command is used to display a list of trusted hosts entered on the Switch using the create trusted_host command above.
Parameters	<ipaddr> – The IP address of the trusted host.
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
-----
10.53.13.94

Total Entries: 1

DES-3026:4#
```

delete trusted_host

delete trusted_host

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

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DES-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
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 Traps      : Enabled
Authenticate Trap : 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#
```

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>

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	<p><i>firmware</i> – Download and install new firmware on the Switch from a TFTP server.</p> <p><i>configuration</i> – Download a switch configuration file from a TFTP server.</p> <p><i><ipaddr></i> – The IP address of the TFTP server.</p> <p><i><path_filename></i> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3024.had.</p> <p><i>increment</i> – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the Switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.</p>
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only administrator-level users can issue this command.

Example usage:

To download a 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	<p><i>configuration</i> – Specifies that the Switch's current settings will be uploaded to the TFTP server.</p> <p><i>log</i> – Specifies that the Switch history log will be uploaded to the TFTP server.</p> <p><ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch.</p> <p><path_filename 64> – Specifies the location of the Switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the Switch.</p>
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only administrator-level users can issue this command.

Example usage:

To upload a 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\setting.txt
Command: upload configuration 10.48.74.121 c:\cfg\setting.txt

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

DES-3026:4#
```

NETWORK MONITORING COMMANDS

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

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

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
```

Frame Size	Frame Counts A	Frames/sec	Frame Type	Total B	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			
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 errors port 3
```

```
Command: show errors port 3
```

```
Port number : 1
```

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

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

show utilization

Purpose	Used to display real-time port utilization statistics.
Syntax	show utilization [cpu ports {<portlist>}]
Description	This command will display the real-time port utilization statistics for the Switch.
Parameters	<i>cpu</i> – Entering this parameter will display the current cpu utilization of the Switch, as a percentage. <i>ports <portlist></i> - Entering this parameter along with a list of ports will display the current utilization of selected ports on the Switch.
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
```

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	<i>index <value_list X-Y></i> – Enter a value that corresponds to an entry made in the log. Multiple entries may be made in the form of <i>x-y</i> , 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 1-4
Command: show log 1-4
Index  Time                               Log Text
-----  -----
4      00000 days 03:03:58  Unit 1, Successful login through Console (Username: Anonymous)
3      00000 days 03:02:58  Unit 1, Logout through Console (Username: Anonymous)
2      00000 days 03:01:28  Unit 1, Successful login through Console (Username: Anonymous)
1      00000 days 03:00:01  Unit 1, Logout through Console (Username: Anonymous)

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

Example usage:

To disable the syslog function on the Switch:

```
DES-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 <int> ipaddress <ipaddr> state [enable disable]}												
Description	The create syslog host command is used to create a new syslog host.												
Parameters	<p><i><index 1-4></i> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p><i>severity</i> – Severity level indicator. These are described in the following:</p> <p>Bold font indicates that the corresponding severity level is currently supported on the Switch.</p> <table border="0"> <thead> <tr> <th>Numerical</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td>Code</td> <td></td> </tr> <tr> <td>0</td> <td>Emergency: system is unusable</td> </tr> <tr> <td>1</td> <td>Alert: action must be taken immediately</td> </tr> <tr> <td>2</td> <td>Critical: critical conditions</td> </tr> <tr> <td>3</td> <td>Error: error conditions</td> </tr> </tbody> </table>	Numerical	Severity	Code		0	Emergency: system is unusable	1	Alert: action must be taken immediately	2	Critical: critical conditions	3	Error: error conditions
Numerical	Severity												
Code													
0	Emergency: system is unusable												
1	Alert: action must be taken immediately												
2	Critical: critical conditions												
3	Error: error conditions												

create syslog host

- 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.

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)

create syslog host**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 <int> ipaddress <ipaddr> state [enable disable]}
Description	The config syslog host command is used to configure the syslog

config syslog host

	protocol to send system log information to a remote host.																																												
Parameters	<p><i>all</i> – Specifies that the command will be applied to all hosts.</p> <p><i><index 1-4></i> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p><i>severity</i> – Severity level indicator. These are described in the following:</p> <p>Bold font indicates that the corresponding severity level is currently supported on the Switch.</p> <table border="0"> <thead> <tr> <th>Numerical</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td>Code</td> <td></td> </tr> <tr> <td>0</td> <td>Emergency: system is unusable</td> </tr> <tr> <td>1</td> <td>Alert: action must be taken immediately</td> </tr> <tr> <td>2</td> <td>Critical: critical conditions</td> </tr> <tr> <td>3</td> <td>Error: error conditions</td> </tr> <tr> <td>4</td> <td>Warning: warning conditions</td> </tr> <tr> <td>5</td> <td>Notice: normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational: informational messages</td> </tr> <tr> <td>7</td> <td>Debug: debug-level messages</td> </tr> </tbody> </table> <p><i>informational</i> – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above.</p> <p><i>warning</i> – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above.</p> <p><i>all</i> – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host.</p> <p><i>facility</i> – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following:</p> <p>Bold font indicates the facility values the Switch currently supports.</p> <table border="0"> <thead> <tr> <th>Numerical</th> <th>Facility</th> </tr> </thead> <tbody> <tr> <td>Code</td> <td></td> </tr> <tr> <td>0</td> <td>kernel messages</td> </tr> <tr> <td>1</td> <td>user-level messages</td> </tr> <tr> <td>2</td> <td>mail system</td> </tr> <tr> <td>3</td> <td>system daemons</td> </tr> <tr> <td>4</td> <td>security/authorization messages</td> </tr> <tr> <td>5</td> <td>messages generated internally by syslog</td> </tr> <tr> <td>6</td> <td>line printer subsystem</td> </tr> <tr> <td>7</td> <td>network news subsystem</td> </tr> <tr> <td>8</td> <td>UUCP subsystem</td> </tr> <tr> <td>9</td> <td>clock daemon</td> </tr> </tbody> </table>	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	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
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																																												
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																																												

config syslog host

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 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#
```

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> fdpdu [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]}
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> fdpdu [enabled disabled]}
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch.
Parameters	<p><i>maxage <value 6-40></i> – 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.</p> <p><i>hellotime <value 1-10></i> – The time interval between transmission of configuration messages by the root device. The default is 2 seconds.</p> <p><i>forwarddelay <value 4-30></i> – The maximum amount of time (in seconds) that the root device will wait before changing states. The default is 15 seconds.</p> <p><i>priority <value 0-61440></i> – 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.</p> <p><i>version [rstp stp]</i> - Select the Spanning Tree Protocol version used for the Switch. For IEEE 802.1d STP select <i>stp</i>. Select <i>rstp</i> for IEEE 802.1w Rapid STP.</p> <p><i>txholdcount <value 1-10></i> - The maximum number of Hello packets transmitted per interval. Default value = 3.</p>

config stp

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	<p><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p><i>cost</i> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is <i>auto</i>.</p> <ul style="list-style-type: none"> <i>auto</i> – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. <i><value 1-200000000></i> - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. <p><i>priority <value 0-240></i> – 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.</p> <p><i>migrate [yes no]</i> – <i>yes</i> 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 (<i>yes</i>) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.</p> <p><i>edge [true false]</i> – <i>true</i> designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is</p>

config stp ports

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.
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

Bridge Parameters Settings
STP Status      : Enabled
Max Age         : 20
Hello Time      : 2
Forward Delay   : 15
Priority        : 32768
STP Version     : STP compatible
TX Hold Count   : 3
Forwarding BPDU : Enabled

Bridge Current Status
Designated Root Bridge : 00-00-51-43-70-00
Root Priority           : 32768
Cost to Root           : 200000
Root Port              : 10
Last Topology Change   : 53sec
Topology Changes Count : 1
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

Bridge Parameters Settings
STP Status       : Disabled
Max Age          : 20
Hello Time       : 2
Forward Delay    : 15
Priority         : 32768
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 STP state of all ports, with STP enabled:

```

DES-3026:4#show stp ports
Command: show stp ports
Port  Connection          State  Cost      Pri  Edge  P2P  Status      Role
-----  -
1     100M/Full/None        Yes    *200000   128  No    Yes   Forwarding  Designated
2     Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
3     Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
4     Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
5     Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
6     Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
7     Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
8     Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
9     Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
10    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
11    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
12    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
13    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
14    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
15    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
16    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
17    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
18    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
19    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
20    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
21    Link Down             Yes    *2000000  128  No    Yes   Disabled    Disabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh

```

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>

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	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be added to the forwarding table.</p> <p>port <port> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a unicast MAC FDB entry:

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

Example usage:

To create 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	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be added to the forwarding table.</p> <p>[add delete] – Add will add the MAC address to the forwarding table. Delete will remove the MAC address from the forwarding table.</p> <p><portlist> – Specifies a port or range of ports to be configured.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

Example usage:

To clear all FDB dynamic entries:

DES-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 multicast_fdb [vlan <vlan_name 32> mac_address <macaddr>]
Description	This command is used to display the current contents of the Switch's multicast MAC address forwarding database.
Parameters	<p><i>vlan <vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i>mac_address <macaddr></i> – The MAC address that will be added to the forwarding table.</p>
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	<p><i>port <port></i> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p> <p><i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i><macaddr></i> – The MAC address that will be added to the forwarding table.</p> <p><i>static</i> – Displays the static MAC address entries.</p> <p><i>aging_time</i> – Displays the aging time for the MAC address forwarding database.</p>
Restrictions	None.

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

```

To display the aging time:

```

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

Unicast MAC Address Aging Time = 5

DES-3026:4#

```

BROADCAST STORM CONTROL COMMANDS

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_groupelist> all] {broadcast [enable disable] multicast [enable disable] dlf [enable disable] threshold <value 64-1024000>}
show traffic control	{group_list <storm_groupelist>}

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_groupelist> all] { broadcast [enabled disabled] multicast [enabled disabled] dlf [enabled disabled] threshold <value 64-1024000> }
Description	This command is used to configure broadcast storm control.
Parameters	<p><i><storm_groupelist></i> – Used to specify a broadcast storm control group. The grouplist corresponds to the port number on the Switch.</p> <p><i>all</i> – Specifies all broadcast storm control groups on the Switch.</p> <p><i>broadcast [enabled disabled]</i> – Enables or disables broadcast storm control.</p> <p><i>multicast [enabled disabled]</i> – Enables or disables multicast storm control.</p> <p><i>dlf [enabled disabled]</i> – Enables or disables dlf traffic control.</p> <p><i>threshold <value 64-1024000></i> – The upper threshold at which the specified traffic control is switched on. The value is the amount of broadcast/multicast/dlf traffic, in Kbps, received by the Switch that will trigger the storm traffic control measures. The value ranges in size from 64 to 1024000 Kbps.</p>
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 enabled
Command: config traffic control all broadcast enabled

Success.

DES-3026:4#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	show traffic control {ports <portlist>}
Description	This command displays the current storm traffic control configuration on the Switch.
Parameters	<i>ports <portlist></i> - Enter a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display traffic control setting for ports 1-5:

```
DES-3026:4#show traffic control group_list 1-5
Command: show traffic control group_list 1-5
```

Group [port]	Threshold (Kbit/sec)	Broadcast Storm	Multicast Storm	Destination Lookup Fail
1	64	Disabled	Disabled	Disabled
2	64	Disabled	Disabled	Disabled
3	64	Disabled	Disabled	Disabled
4	64	Disabled	Disabled	Disabled
5	64	Disabled	Disabled	Disabled

```
Total Entries: 5
DES-3026:4#
```

QoS COMMANDS

The DES-3026 switch supports 802.1p priority queuing. 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 Q0 class.
- Priority 1 is assigned to the Switch's Q0 class.
- Priority 2 is assigned to the Switch's Q1 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.

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.

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

Command	Parameters
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>}

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

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	<p>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 <u>only if</u> 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.</p> <p>The default settings for QoS scheduling employ this strict priority scheme to empty priority classes of service.</p> <p>The config scheduling command can be used to specify the round robin rotation by which these four hardware priority classes of service are reduced.</p> <p>The weight parameter allows you to specify 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 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.</p>

config scheduling

Parameters	<p><i><class_id></i> – 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.</p> <p><i>weight <value 1-55></i> – 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:</p> <table border="1"> <thead> <tr> <th>Class</th> <th>Weight</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>1</td> </tr> <tr> <td>1</td> <td>2</td> </tr> <tr> <td>2</td> <td>4</td> </tr> <tr> <td>3</td> <td>8</td> </tr> </tbody> </table>	Class	Weight	0	1	1	2	2	4	3	8
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	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3

Parameters **<priority 0-7>** – Specifies which of the eight 802.1p priority values (0 through 7) you want to map to one of the Switch's hardware priority classes of service (<class_id>, 0 through 3).

<class_id 0-3> – Specifies which of the Switch's hardware priority classes of service the 802.1p priority value (specified above) will be mapped to.

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-0>
Priority-1 -> <Class-0>
Priority-2 -> <Class-1>
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 you to specify the 802.1p priority value an untagged, incoming packet will be assigned before being forwarded to its destination.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Specifies that the config 802.1p default_priority command will be applied to all ports on the Switch.</p> <p><i><priority 0-7></i> – Specifies the 802.1p priority value that an untagged, incoming packet will be given before being forwarded to its destination.</p>

config 802.1p default_priority

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	<p>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 contains four hardware priority classes of service. Incoming packets must be mapped to one of these four hardware priority classes of service. This command is used to specify the rotation by which these four hardware priority classes of service are emptied.</p> <p>The Switch's default is to empty the four priority classes of service in order – from the highest priority class of service (queue 3) to the lowest priority class of service (queue 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority class of service to transmit its packets. Lower classes of service will be pre-empted from emptying its queue if a packet is received on a higher class of service. The packet that was received on the highest class of service will transmit its packet before allowing the lower class to resume clearing its queue.</p>
Parameters	<p><i>strict</i> – 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.</p> <p><i>weight_fair</i> – 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.</p>
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	<p><portlist> – Specifies a port or range of ports to be configured for bandwidth control.</p> <p><i>rx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <value 64-1024000>) will be applied to the rate at which the above specified ports will be allowed to receive packets</p> <ul style="list-style-type: none"> ▪ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ <value 64-1024000> – Specifies the packet limit, in kbps, that the above ports will be allowed to receive. <p><i>tx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <value 64-1024000>) will be applied to the rate at which the above specified ports will be allowed to transmit packets.</p> <ul style="list-style-type: none"> ▪ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets 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.
---------	--

show bandwidth_control

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#
```

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	<p><portlist> – Specifies a port or range of ports to be configured for traffic segmentation.</p> <p>forward_list – Specifies a port or range of ports that will receive forwarded frames from the ports specified in the portlist, above.</p> <ul style="list-style-type: none"> • null – No ports are specified • <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

show traffic_segmentation

	current traffic segmentation configuration on the Switch.
Parameters	<portlist> – Specifies a port or range of ports for which the current traffic segmentation configuration on the Switch will be displayed.
Restrictions	The port lists for segmentation and the forward list must be on the same switch.

Example usage:

To display the current traffic segmentation configuration on the Switch.

```

DES-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

```

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 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	<p><i>port <port></i> – This specifies the Target port (the port where mirrored packets will be sent).</p> <p><i>add source ports</i> – The port or ports being mirrored. This cannot include the Target port.</p> <ul style="list-style-type: none"> ▪ <i><portlist></i> – 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. <i>rx</i> – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list. <i>tx</i> – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list. <i>both</i> – 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 source port 1 ingress_target port 2
egress_target port 3
Command: config mirror source port 1 ingress_target port 2 egress_target
port 3

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 you to enter a port mirroring configuration into the Switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	None.

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 you to enter a port mirroring configuration into the Switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DES-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 for Ingress : 2
Target Port for Egress  : 3
Mirrored Port      : 1

DES-3026:4#
```

VLAN COMMANDS

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

Command	Parameters
create vlan	<vlan_name 32> {tag <vlanid 1-4094>}
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 1-4094>}
Description	This command allows the creation of a VLAN on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN to be created.</p> <p>tag <vlanid 1-4094> – The VLAN ID of the VLAN to be created. Allowed values = 1-4094</p>
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 a 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	<p><i><vlan_name 32></i> – The name of the VLAN to add ports to.</p> <p><i>add</i> – Specifies to add ports to a previously created vlan.</p> <p><i>delete</i> – Specifies to delete ports to a previously created vlan.</p> <p><i>tagged</i> – Specifies the additional ports as tagged.</p> <p><i>untagged</i> – Specifies the additional ports as untagged.</p> <p><i><portlist></i> – A port or range of ports to be added to or deleted from the VLAN.</p>
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	<i><vlan_name 32></i> – 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
Untagged ports : 1-26

Total Entries : 1

DES-3026:4#
```

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	<p><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.</p> <p>type – Specify the type of link aggregation used for the group. If the type is not specified the default type is static.</p> <ul style="list-style-type: none"> ▪ 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 you to configure a link aggregation group that was created with the create link_aggregation command above.
Parameters	<p><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.</p> <p><i>master port <port></i> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.</p> <p><i>ports <portlist></i> – Specifies a port or range of ports that will belong to the link aggregation group. Ports may be listed in only one port aggregation group, that is, link aggregation groups may not overlap.</p> <p><i>state [enable disable]</i> – Allows the user to enable or disable the specified link aggregation group.</p>

config link_aggregation

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/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	<p><i>mac_source</i> – Indicates that the Switch should examine the MAC source address.</p> <p><i>mac_destination</i> – Indicates that the Switch should examine the MAC destination address.</p> <p><i>mac_source_dest</i> – Indicates that the Switch should examine the MAC source and destination addresses</p>
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

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	<p><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 cannot be viewed here.</p> <p><i>algorithm</i> – Displays the link aggregation algorithm in use on the Switch.</p>
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

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

Group ID      : 1
Type          : Trunk
Master Port   : 5
Member Port   : 5-7,9
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 Algoritm = 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	<p><portlist> – Specifies a range of ports to be configured for LACP.</p> <p><i>mode</i> – Select the mode to determine if LACP ports will process LACP control frames.</p> <ul style="list-style-type: none"> ▪ <i>active</i> – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be

config lacp_ports

changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

- *passive* – LACP ports that are designated as passive cannot process LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have “active” LACP ports (see above).

Restrictions Only administrator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DES-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	Only administrator-level users can issue this command.

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#
```

BASIC IP COMMANDS

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

Command	Parameters
config ipif	<ipif_name 12> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable]} bootp dhcp]
show ipif	{<ipif_name 12>}

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

config ipif	
Purpose	Used to configure the System IP interface.
Syntax	config <ipif_name 12> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable]} bootp dhcp]
Description	This command is used to configure the System IP interface on the Switch.
Parameters	<p><i><ipif_name 12></i> - 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.</p> <p><i><network_address></i> – 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).</p> <p><i><vlan_name 32></i> – The name of the VLAN corresponding to the System IP interface.</p> <p><i>state [enable disable]</i> – Used to enable or disable the IP interface.</p> <p><i>bootp</i> – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface.</p> <p><i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface.</p>
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 {<ipif_name 12>}
Description	This command will display the configuration of an IP interface on the Switch.
Parameters	<ipif_name 12> - Enter the name of the IP interface for which to view the settings. (System)
Restrictions	None.

Example usage:

To display IP interface settings.

```
DES-3026:4#show ipif System
Command: show ipif System

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

DES-3026:4#
```

IGMP SNOOPING COMMANDS

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

Command	Parameters
config igmp_snooping	[<vlan_name 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 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 [enabled disabled]}
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 32> all] {host_timeout <sec 1-16711450> router_timeout <sec 1-16711450> leave_timer <sec 0-16711450> state [enable disable] fast_leave [enable disable]}
Description	This command allows the user to configure IGMP snooping on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p><i>all</i> – Selecting this parameter will configure IGMP for all VLANs on the Switch.</p> <p><i>host_timeout</i> <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.</p> <p><i>router_timeout</i> <sec 0-16711450> – 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.</p> <p><i>leave_timer</i> <sec 0-16711450> – Leave timer. The default is 2 seconds.</p> <p><i>state</i> [enable disable] – Allows the user to enable or disable IGMP snooping for the specified VLAN.</p> <p><i>fast_leave</i> [enable disable] – This parameter allows the user to enable the <i>fast leave</i> function. Enabled, this function will allow members of a multicast</p>

config igmp_snooping

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 default host_timeout 250 state enabled
Command: config igmp_snooping default host_timeout 250 state enabled
```

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 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 [enabled disabled]}
Description	This command configures IGMP snooping querier.
Parameters	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured.</p> <p><i>all</i> – Selecting this parameter will configure IGMP for all VLANs on the Switch.</p> <p><i>query_interval</i> <sec 1-65535> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p><i>max_response_time</i> <sec 1-25> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.</p> <p><i>robustness_variable</i> <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:</p> <ul style="list-style-type: none"> • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. Users may wish to

config igmp_snooping querier

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 [*enabled* | *disabled*] – 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 default query_interval 125 state enabled
Command: config igmp_snooping querier default query_interval 125 state enabled

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	<p><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p>[<i>add</i> <i>delete</i>] – Specify whether to add or delete ports defined in the following parameter <portlist>, to the router port function.</p> <p><portlist> – Specifies a port or range of ports that will be configured as router ports.</p>
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	<i>forward_mcrouter_only</i> – 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	<p><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p><i>static</i> – Displays router ports that have been statically configured.</p> <p><i>dynamic</i> – Displays router ports that have been dynamically configured.</p>
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#
```

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>

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



NOTE: The uplink module ports (DES-3010F/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	<p><i>ports</i> <portlist> – Specifies a port or range of ports to be configured for port security.</p> <p><i>all</i> – Configure port security for all ports on the Switch.</p> <p><i>admin_state</i> [enable disable] – Enable or disable port security for the listed ports.</p> <p><i>max_learning_addr</i> <max_lock_no 0-10> - Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p><i>lock_address_mode</i> [Permanent DeleteOnTimeout DeleteOnReset] – Indicates the method of locking addresses. The user has three choices:</p> <ul style="list-style-type: none"> ▪ <i>Permanent</i> – The locked addresses will not age out after the aging timer expires. ▪ <i>DeleteOnTimeout</i> – The locked addresses will age out after the aging timer expires. ▪ <i>DeleteOnReset</i> – The locked addresses will not age out until the Switch has been reset.

config port_security ports

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	<i>ports <portlist></i> – 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 1-19
Command: show port_security ports 1-19
```

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
9	Disabled	1	DeleteOnReset
10	Disabled	1	DeleteOnReset
11	Disabled	1	DeleteOnReset
12	Disabled	1	DeleteOnReset
13	Disabled	1	DeleteOnReset
14	Disabled	1	DeleteOnReset
15	Disabled	1	DeleteOnReset
16	Disabled	1	DeleteOnReset
17	Disabled	1	DeleteOnReset
18	Disabled	1	DeleteOnReset
19	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	<i>vlan_name <vlan_name 32></i> - Enter the corresponding VLAN of the entry to delete. <i>mac_address <macaddr></i> - Enter the corresponding MAC address of the entry to delete. <i>port <port></i> - 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	<i><portlist></i> – 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#
```

802.1X COMMANDS

The DES-3026 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 1-999999999> 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>
show 802.1x user	
show acct_client	
show auth_client	
show auth_diagnostics	{ports [<portlist> all]}
show auth_session_+statistics	{ports [<portlist> all]}

Command	Parameters
show auth_statistics	{ports [<portlist> all]}

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



NOTE: The uplink module ports (DES-3010F/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	<i>[port_based mac_based ports]</i> – 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	<p>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.</p> <p>The following details what is displayed:</p> <p>Port number – Shows the physical port number on the Switch, in port-based mode only.</p> <p>MAC Address – Displays the MAC address of the Switch in MAC-based mode only.</p> <p>Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE.</p> <p>Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout – Shows the current state of the Backend Authenticator.</p> <p>Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.</p>
Parameters	<i>ports <portlist></i> – 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	<p>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.</p> <p>The following details what is displayed:</p> <p>802.1x Enabled/Disabled – Shows the current status of 802.1x functions on the Switch.</p> <p>Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the Switch and a RADIUS server.</p> <p>Port number – Shows the physical port number on the Switch.</p> <p>Capability: Authenticator/None – Shows the capability of 802.1x functions on the port number displayed above. There are four 802.1x capabilities that can be set on the Switch: Authenticator, Supplicant, Authenticator and Supplicant, and None.</p> <p>Port Status: Authorized/Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not</p>

show 802.1x auth_configuration

authenticated, and can not access the network.

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 – 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
Port Status      : Authorized
PAE State        : ForceAuth
Backend State    : Success
AdminCrIDir     : Both
OpenCrIDir      : Both
Port Control     : Auto
QuietPeriod      : 60 sec
TxPeriod         : 30 sec
SuppTimeout     : 30 sec
ServerTimeout   : 30 sec
MaxReq          : 2 times
ReAuthPeriod    : 3600 sec
ReAuthenticate   : Disabled
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry
a All

```

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	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>authenticator</i> – A user must pass the authentication process to gain access to the network.</p> <p><i>none</i> – The port is not controlled by the 802.1x functions.</p>
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	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>default</i> – Returns all of the ports in the specified range to their 802.1x default settings.</p> <p><i>direction [both in]</i> – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.</p> <p><i>port_control</i> – Configures the administrative control over the authentication process for the range of ports.</p> <ul style="list-style-type: none"> ▪ <i>force_auth</i> – Forces the Authenticator for the port to become authorized. Network access is allowed. ▪ <i>auto</i> – Allows the port's status to reflect the outcome of the authentication process. ▪ <i>force_unauth</i> – Forces the Authenticator for the port to become unauthorized. Network access will be blocked. <p><i>quiet_period <sec 0-65535></i> – Configures the time interval between authentication failure and the start of a new authentication attempt.</p> <p><i>tx_period <sec 1-65535></i> - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.</p> <p><i>supp_timeout <sec 1-65535></i> - Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.</p> <p><i>server_timeout <sec 1-65535></i> - Configure the length of time to wait for a response from a RADIUS server.</p> <p><i>max_req <value 1-10></i> – Configures the number of times to retry sending packets to a supplicant (user).</p> <p><i>reauth_period <sec 1-65535></i> – Configures the time interval between successive re-authentications.</p> <p><i>enable_reauth [enable disable]</i> – Determines whether or not the Switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication parameters for ports 1 – 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	<i>[local radius_eap]</i> – 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	<p><i>port_based ports</i> – This instructs the Switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified.</p> <ul style="list-style-type: none"> ▪ <i><portlist></i> – Specifies a port or range of ports to be initialized. ▪ <i>all</i> – Specifies all of the ports on the Switch to be initialized. <p><i>mac_based</i> - 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.</p> <ul style="list-style-type: none"> ▪ <i>ports <portlist></i> – Specifies a port or range of ports. ▪ <i>all</i> – Specifies all of the ports on the Switch. <p><i>mac_address <macaddr></i> - Specifies the MAC address of the client to be added.</p>
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	<p><i>port_based</i> – 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.</p> <ul style="list-style-type: none"> ▪ <i>ports <portlist></i> – Specifies a port or range of ports to be reauthorized. ▪ <i>all</i> – Specifies all of the ports on the Switch to be reauthorized. <p><i>mac-based</i> - 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.</p> <ul style="list-style-type: none"> ▪ <i>ports <portlist></i> – Specifies a port or range of ports. ▪ <i>all</i> – Specifies all ports on the Switch. <p><i>mac_address <macaddr></i> - Specifies the MAC address of the client to add.</p>
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	<p><i><server_index 1-3></i> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the Switch.</p> <p><i><server_ip></i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.</p> <ul style="list-style-type: none"> ▪ <i><passwd 32></i> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. <p><i>default</i> – Returns all of the ports in the range to their default RADIUS settings.</p> <p><i>auth_port <udp_port_number 1-65535></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number 1-65535></i> – The UDP port number for accounting requests. The default is 1813.</p>
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	<i><server_index 1-3></i> – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch.
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	<p><i><server_index 1-3></i> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the Switch.</p> <p><i><server_ip></i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.</p> <ul style="list-style-type: none"> ▪ <i><passwd 32></i> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. <p><i>default</i> – Returns all of the ports in the range to their default RADIUS settings.</p> <p><i>auth_port <udp_port_number 1-65535></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number 1-65535></i> – The UDP port number for accounting requests. The default is 1813.</p>
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
-----  -
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>
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.
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	<i>ports <portlist></i> – 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	<i>ports <portlist></i> – Specifies a port or range of ports to be viewed. <i>all</i> – 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	<i>ports <portlist></i> – 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
```

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	<p><i>primary</i> – This is the primary server the SNTP information will be taken from.</p> <ul style="list-style-type: none"> ▪ <ipaddr> – The IP address of the primary server. <p><i>secondary</i> – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <ul style="list-style-type: none"> ▪ <ipaddr> – The IP address for the secondary server. <p><i>poll-interval</i> – This is the interval between requests for updated SNTP information.</p> <ul style="list-style-type: none"> ▪ <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	Only administrator-level users can issue this command.

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 <code>config sntp</code>). 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 ddmthyyy> <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	<p><i>date</i> – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003.</p> <p><i>time</i> – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.</p>
Restrictions	Only administrator-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.
Parameters	<p><i>operator</i> – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT.</p> <p><i>hour</i> – Select the number hours offset from GMT (Greenwich Mean Time).</p> <p><i>min</i> – Select the number of minutes difference added or subtracted to adjust the time zone.</p>
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	<p><i>disable</i> - Disable the DST seasonal time adjustment for the Switch.</p> <p><i>repeating</i> - 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.</p> <p><i>annual</i> - 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.</p> <p><i>s_week</i> - Configure the week of the month in which DST begins.</p>

config dst

- *<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)
- 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_day tue s_mth 4 s_time
15:00 e_week 2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time
15:00 e_week 2 e_day wed e_mth 10 e_time 15:30 offset 30
```

Success.

```
DES-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	Only administrator-level users can issue this command.

Example usage:

To show the time settings:

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

Current Time Source : System Clock
Current Time       : 0 Days 06:47:52
Time Zone         : GMT +02:30
Daylight Saving Time : Repeating
Offset in Minutes  : 30
  Repeating From   : Apr 2nd Tue 15:00
                  To   : Oct 2nd Wed 15:30
  Annual From     : 29 Apr 00:00
                  To   : 12 Oct 00:00

DES-3026:4#
```

ROUTING TABLE COMMANDS

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

Command	Parameters
create iproute	[default] <ipaddr> {<metric 1-65535>}
delete iproute	[default]
show iproute	{<network address>} {static}

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

create iproute	
Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	create iproute [default] <ipaddr> {<metric 1-65535>}
Description	This command is used to create a default static IP route entry to the Switch's IP routing table.
Parameters	<p><ipaddr> – The gateway IP address for the next hop router.</p> <p><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.</p>
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	<i>network address</i> – 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). <i>static</i> - 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#
```

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 arprentry	{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 arprentry

Purpose	Used to display the ARP table.
Syntax	show arprentry {ipif <ipif_name 12> ipaddress <ipaddr> [static]}
Description	This command is used to display the current contents of the Switch's ARP table.
Parameters	<p><ipif_name 12> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on.</p> <p><ipaddr> – The network address corresponding to the IP interface name above.</p> <p>static – Displays the static entries to the ARP table.</p>
Restrictions	None.

Example Usage:

To display the ARP table:

```

DES-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	<i>time</i> <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#
```

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 as 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.

The DES-3026 can be used as a member switch (MS) of an SIM group only and has a default setting of candidate. It has no configurations for commander switch functions and therefore cannot be a commander switch of a SIM group. 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-3026 as a member switch. For more information on adding the DES-3026 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	
config sim	[candidate dp_interval <sec 30-90> hold_time <sec 100-255>]

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
Description	<p>This command will display the current information regarding the SIM group on the Switch, including the following:</p> <p>SIM Version - Displays the current Single IP Management version on the Switch.</p> <p>Firmware Version - Displays the current Firmware version on the Switch.</p> <p>Device Name - Displays the user-defined device name on the Switch.</p> <p>MAC Address - Displays the MAC Address of the Switch.</p> <p>Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3).</p> <p>Platform – Switch Description including name and model number.</p> <p>SIM State –Displays the current Single IP Management State of the Switch, whether it be enabled or disabled.</p> <p>Role State – Displays the current role the Switch is taking, including Commander or Member. A stand-alone switch will always have the candidate role.</p> <p>Discovery Interval - Time in seconds the Switch will send discovery packets out over the network.</p>

show sim

	Hold time – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.
Parameters	None.
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-1.50
Firmware Version : 1.01.005
Device Name      :
MAC Address      : 00-35-26-11-11-00
Capabilities     : L2
Platform         : DES-3026 L2 Switch
SIM State        : Enabled
Role State       : Candidate
Discovery Interval : 30 sec
Hold Time        : 100 sec

DES-3026:4#
```

To show the switch sim settings after being added to the SIM group:

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

SIM Version      : VER-1.50
Firmware Version : 1.01.005
Device Name      :
MAC Address      : 00-35-26-11-11-00
Capabilities     : L2
Platform         : DES-3026 L2 Switch
SIM State        : Enabled
Role State       : Member
Discovery Interval : 30 sec
Hold Time        : 100 sec
-----CS Info-----
CS Group Name    : default
CS MAC Addr     : 00-53-10-08-00-00
CS Holdtime     : 90s

DES-3026:4#
```

config sim

Purpose	Used to configure role parameters for the SIM protocol on the Switch.
Syntax	config sim [candidate] dp_interval <30-90> hold_time <sec 100-255>]
Description	This command is used to configure parameters of switches of the SIM.
Parameters	<p><i>candidate</i> – Used to change the role of a commander switch to a candidate switch.</p> <p><i>dp_interval <30-90></i> – 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.</p> <p><i>hold time <sec 100-255></i> – 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.</p>
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 candidate dp_interval 30
Command:config sim candidate dp_interval 30

Success.

DES-3026:4#
```

To change the hold time of the discovery protocol:

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

Success.

DES-3026:4#
```

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
?	
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
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config account
config arp_aging time
config arpentry
config command history
config dst
config fdb_aging_time minutes
config gvrp
config igmp snooping
```

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 32> | all] {host_timeout <sec 1-16711450> | router_timeout
<sec 1-16711450> | leave_timer <sec 0-16711450> | 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 init
config 802.1x reauth
config account
config arp_aging time
config bandwidth_control
config command history
config dst
config fdb aging_time minutes
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#
```

TECHNICAL SPECIFICATIONS

Physical and Environmental	
AC input & External Redundant power Supply:	100 – 120; 200 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	DES-3010F – 10.7W DES-3010G – 9.9W DES-3018 – 10.5W DES-3026 – 11.6W
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/G – 1.5kg DES-3018 and DES-3026 - 2.1 kg
EMI:	FCC Class A, CE Class A, C-Tick 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:	<table border="0"> <tr> <td></td> <td>Half-duplex</td> <td>Full-duplex</td> </tr> <tr> <td>Ethernet</td> <td>10 Mbps</td> <td>20Mbps</td> </tr> <tr> <td>Fast Ethernet</td> <td>100Mbps</td> <td>200Mbps</td> </tr> <tr> <td>Gigabit Ethernet</td> <td>n/a</td> <td>2000Mbps</td> </tr> </table>		Half-duplex	Full-duplex	Ethernet	10 Mbps	20Mbps	Fast Ethernet	100Mbps	200Mbps	Gigabit Ethernet	n/a	2000Mbps
	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 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-3026 - 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 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.