D-Link®

DES-3250TG

48 10/100Mbps plus 2 Gigabit Ports

Layer 2 Stackable Switch

Command Line Interface Reference Manual

Release 4

March 2005 P/N 651TG3250055

Table of Contents

1

INTRODUCTION

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

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

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**
- **no flow control**

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

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

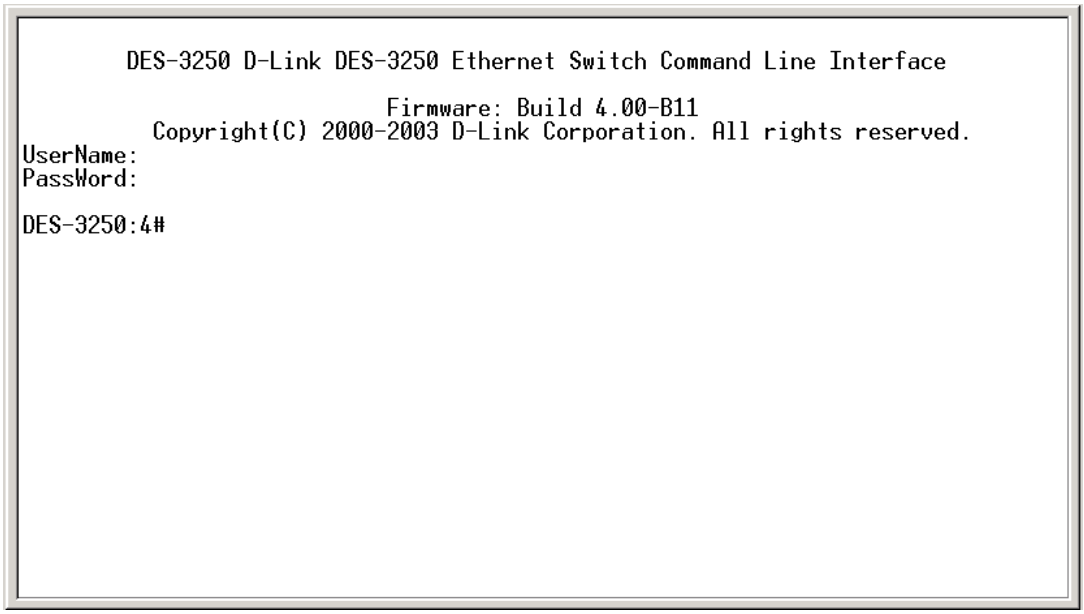

Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-3250:4#**. 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.

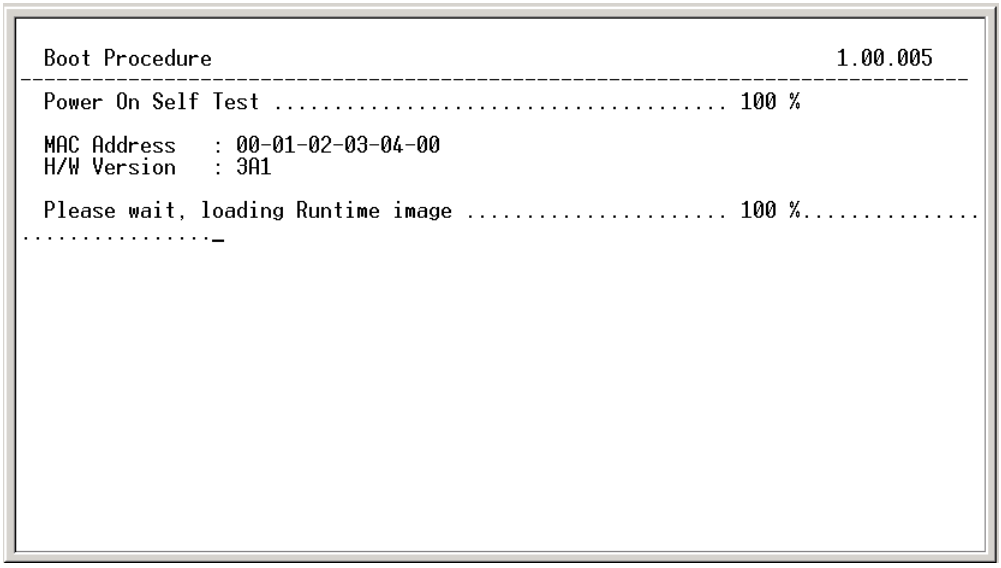

Figure 1-2. Boot Screen

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

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

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

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.

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

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

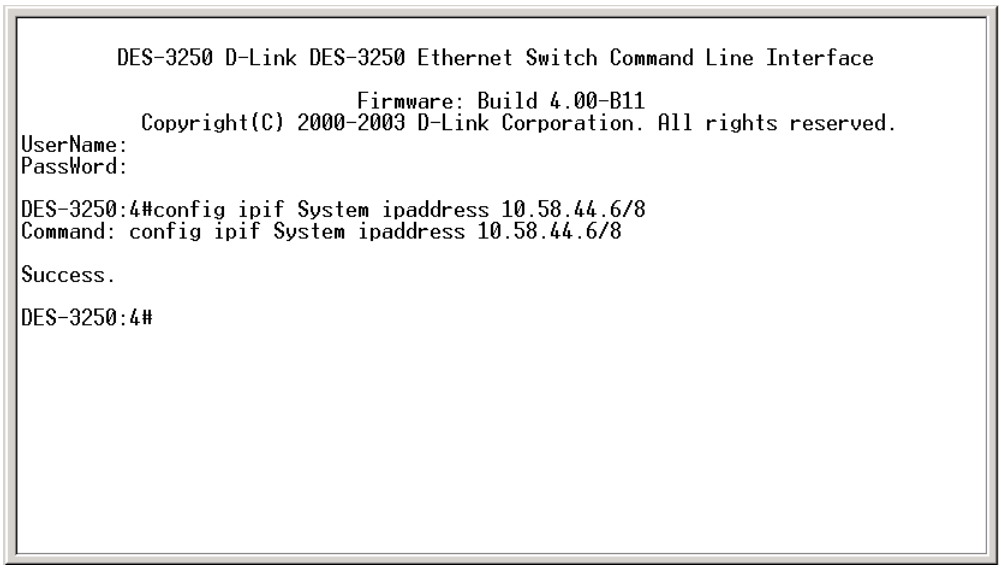

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.58.44.6 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet, SNMP MIB browser and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

2

USING THE CONSOLE CLI

The DES-3250TG supports a console management interface that allows the user to connect to the Switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the Switch to use an SNMP-based network management software over the network.

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

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

Connecting to the Switch

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

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

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

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

```
        DES-3250 D-Link DES-3250 Ethernet Switch Command Line Interface

                              Firmware: Build 4.00-B11
          Copyright(C) 2000-2003 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DES-3250:4#
```

Figure 2-1. Initial Console Screen

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

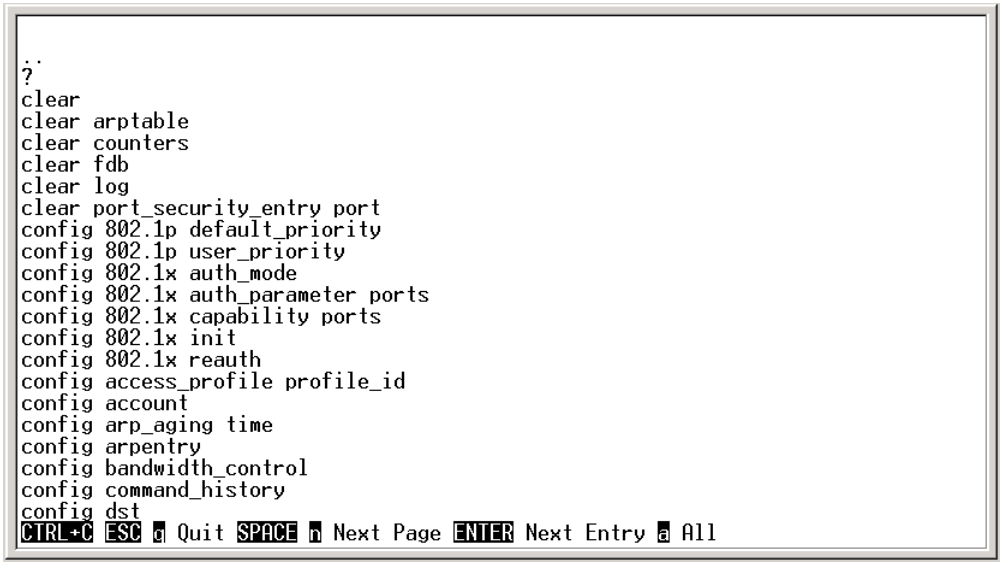

Figure 2-2. The ? Command

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

Figure 2-3. Example Command Parameter Help

In this case, the command **config account** was entered without the parameter **<username>**. The CLI will then prompt you to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

In addition, after typing any given command plus one space, you can see all of the next possible sub-commands, in sequential order, by repeatedly pressing the **Tab** key.

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

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

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

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

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

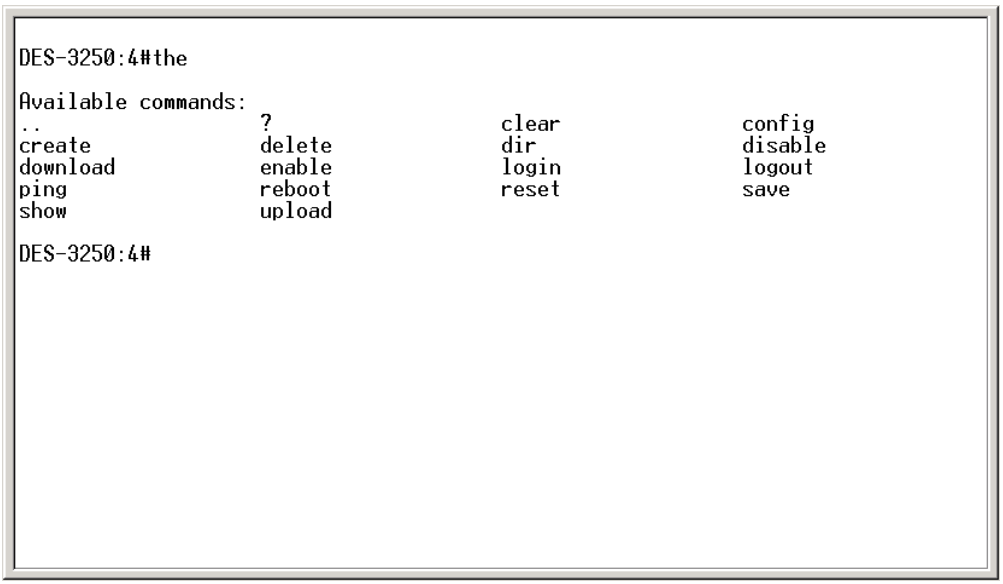

Figure 2-5. The Next Available Commands Prompt

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.

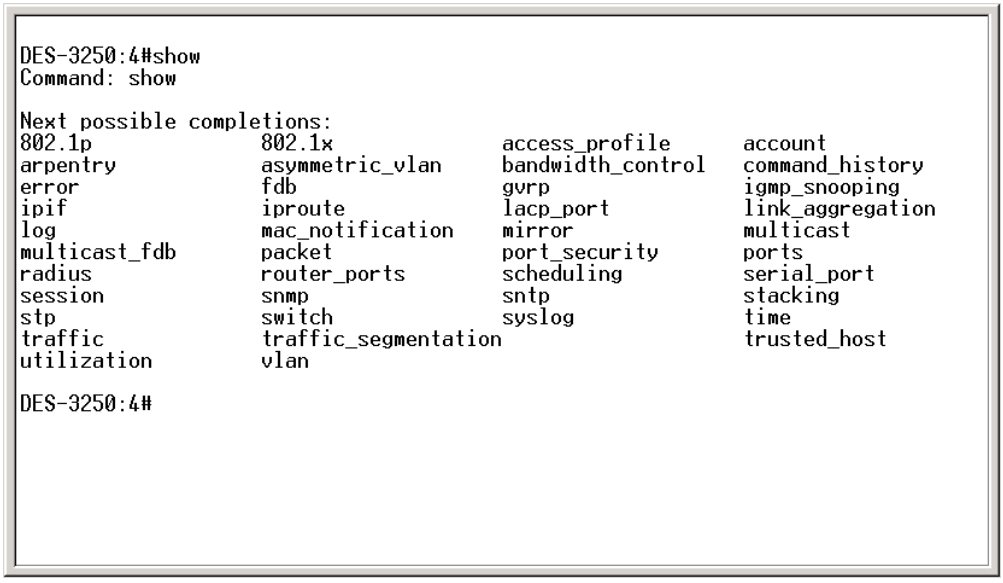

Figure 2-6. Next possible completions: Show Command

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

3

COMMAND SYNTAX

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

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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**create ipif <ipif_name> vlan <vlan_name 32> ipaddress <network_address>**
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	**create ipif Engineering vlan Design ipaddress 10.24.22.5/255.0.0.0**

[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 snmp [community | detail]**
Description	In the above syntax example, you must specify either **community,** or **detail**. Do not type the backslash.
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 following chapter, Basic Commands for more details about the reset command.
Example command	**reset config**

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

Multiple Page Display Control Keys	
Space	Displays the next page.
CTRL+c	Stops the display of remaining pages when multiple pages are to be displayed.
ESC	Stops the display of remaining pages when multiple pages are to be displayed.
n	Displays the next page.
p	Displays the previous page.
q	Stops the display of remaining pages when multiple pages are to

	be displayed.
r	Refreshes the pages currently displayed.
a	Displays the remaining pages without pausing between pages.
Enter	Displays the next line or table entry.

4

BASIC SWITCH COMMANDS

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

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

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	*admin <username>* *user <username>*

create account	
Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.

Example usage:

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

```
DES-3250:4#create account admin dlink
Command: create account admin dlink

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

Success.

DES-3250:4#
```

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-3250:4#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-3250:4#
```

show account

Purpose	Used to display user accounts
Syntax	**show account**
Description	Displays all user accounts created on the Switch. Up to 8 user accounts can exist at one time.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the accounts that have been created:

```
DES-3250:4#show account
Command: show account

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

Total Entries: 1

DES-3250:4#
```

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-3250:4#delete account System
```

```
Command: delete account System

Success.

DES-3250:4#
```

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-3250:4#show session
Command: show session
ID  Live Time       From          Level   Name
---  ------------    ------------   -----   --------
8   23:59:21.450   Serial Port   4       Anonymous
```

show switch

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

Example usage:

To display the Switch's information:

```
DES-3250:4#show switch
Command: show switch
```

```
Device Type            : DES-3250TG Fast-Ethernet Switch
Ext. Ports             : 1000TX + 1000TX
MAC Address            : 00-01-02-03-04-00
IP Address             : 10.58.44.4 (Manual)
VLAN Name              : default
Subnet Mask            : 255.0.0.0
Default Gateway        : 0.0.0.0
Boot PROM Version      : Build 1.00.005
Firmware Version       : Build 4.00-B11
Hardware Version       : 3A1
Device S/N             :
System Name            :
System Location        :
System Contact         :
Spanning Tree          : Disabled
GVRP                   : Disabled
IGMP Snooping          : Disabled
TELNET                 : Enabled (TCP 23)
WEB                    : Enabled (TCP 80)
RMON                   : Disabled
Asymmetric VLAN        : Disabled

DES-3250:4#

DES-3250:4#
```

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-3250:4#show serial_port
Command: show serial_port

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

DES-3250:4#
```

config serial_port

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

Example usage:

To configure baud rate:

```
DES-3250:4#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

DES-3250:4#
```

enable clipaging

Purpose	Used to pause the scrolling of the console screen when the show command displays more than one page.
Syntax	**enable clipaging**
Description	This command is used when issuing the show 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:

```
DES-3250:4#enable clipaging
Command: enable clipaging

Success.

DES-3250:4#
```

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when the show 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:

```
DES-3250:4#disable clipaging
Command: disable clipaging

Success.

DES-3250:4#
```

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

Example usage:

To enable Telnet and configure port number:

```
DES-3250:4#enable telnet 23
Command: enable telnet 23

 Success.

DES-3250:4#
```

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-3250:4#disable telnet
Command: disable telnet

Success.

DES-3250:4#
```

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	*<tcp_port_number 1-65535>* – The TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" port for the Web-based management software is 80.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DES-3250:4#enable web 80
Command: enable web 80

Success.

DES-3250:4#
```

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-3250:4#disable web
Command: disable web

Success.

DES-3250:4#
```

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-3250:4#save
Command: save

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

DES-3250:4#
```

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-3250:4#reboot
Command: reboot
Are you sure want to proceed with the system reboot? (y|n)
Please wait, the switch is rebooting...
```

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	*config* – If the keyword 'config' is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, and the switch history log. The Switch will not save or reboot. *system* – If the keyword 'system' is specified all of the factory default settings are restored on the Switch. The Switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base. If no parameter is specified, the Switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The Switch will not save or reboot.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3250:4#reset config
Command: reset config
Are you sure to proceed with system reset?(y / n)
Success.

DES-3250:4#
```

login

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

Example usage:

To initiate the login procedure:

```
DES-3250:4#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-3250:4#logout
```

5

SWITCH PORT COMMANDS

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

Command	Parameters
config ports	[<portlist | all> speed [auto | 10_half | 10_full |100_half | 100_full | 1000_full} | flow_control [enable | disable] | learning [enable | disable] state [enable | disable]} description <pdesc 32>
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} | flow_control [enable | disable] | learning [enable | disable] state [enable | disable]} description <pdesc 32>**

Description This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the <*portlist*> will be affected.

Parameters *all* – Configure all ports on the Switch.

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

speed – Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following:

- *auto* – Enables auto-negotiation for the specified range of ports.
- *[10 | 100 | 1000]* – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 and cannot be set to slower speeds.
- *[half | full]* – Configures the specified range of ports as either full-duplex or half-duplex.

flow_control [enable | disable] – Enable or disable flow control for the specified ports.

learning [enable | disable] – Enables or disables the MAC address learning on the specified range of ports.

state [enable | disable] – Enables or disables the specified range of ports

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

Restrictions Only administrator-level users can issue this command.

Example usage:

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

```
DES-3250:4#config ports 1-3 speed 10_full learning enable state
enable

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


Success.


DES-3250:4#
```

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 **show ports** command indicates that a previously entered port description will be included in the display.
Restrictions	None.

Example usage:

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

```
DES-3250:4#show ports
Command: show ports

Port   Port       Settings          Connection        Address
       State      Speed/Duplex      Speed/Duplex      Learning
----   --------   ----------------  ----------------  ----------------
1      Enabled    Auto              100M/Full/None    Enabled
2      Enabled    Auto              Link Down         Enabled
3      Enabled    Auto              Link Down         Enabled
4      Enabled    Auto              Link Down         Enabled
5      Enabled    Auto              Link Down         Enabled
6      Enabled    Auto              Link Down         Enabled
7      Enabled    Auto              Link Down         Enabled
8      Enabled    Auto              Link Down         Enabled
9      Enabled    Auto              100M/Full/None    Enabled
10     Enabled    Auto              Link Down         Enabled
11     Enabled    Auto              Link Down         Enabled
12     Enabled    Auto              Link Down         Enabled
13     Enabled    Auto              Link Down         Enabled
14     Enabled    Auto              Link Down         Enabled
```

```
 15  Enabled    Auto                Link Down           Enabled
 16  Enabled    Auto                Link Down           Enabled
 17  Enabled    Auto                Link Down           Enabled
 18  Enabled    Auto                Link Down           Enabled
 19  Enabled    Auto                Link Down           Enabled
 20  Enabled    Auto                Link Down
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Example usage:

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

```
DES-3250:4#show ports description
Command: show ports description

Port  Port       Settings                Connection              Address
      State      Speed/Duplex            Speed/Duplex            Learning
------ --------  ---------------------   ---------------------   --------
1     Enabled    Auto/Disabled           Link Down               Enabled
 Description: dads1
2     Enabled    Auto/Disabled           Link Down               Enabled
 Description:
3     Enabled    Auto/Disabled           Link Down               Enabled
 Description:
4     Enabled    Auto/Disabled           Link Down               Enabled
 Description:
5     Enabled    Auto/Disabled           Link Down               Enabled
 Description:
6     Enabled    Auto/Disabled           Link Down               Enabled
 Description:
7     Enabled    Auto/Disabled           Link Down               Enabled
 Description:
8     Enabled    Auto/Disabled           Link Down               Enabled
 Description:
9     Enabled    Auto/Disabled           Link Down               Enabled
 Description:
10    Enabled    Auto/Disabled           Link Down               Enabled
 Description:
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

6

PORT SECURITY COMMANDS

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

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

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

config port_security ports

Purpose Used to configure port security settings.

Syntax **config port_security ports [<portlist> | all] {admin_state [enable| disable] | max_learning_addr <max_lock_no 0-10> | 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 affected.

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

all – Configure port security for all ports on the Switch.

admin_state [enable | disable] – Enable or disable port security for the listed ports.

max_learning_addr <max_lock_no 0-10> - Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.

lock_address_mode [Permanent | DeleteOnTimout | DeleteOnReset] – Indicates the method of locking addresses. The user has three choices:

- *Permanent* – The locked addresses will not age out after the aging timer expires.
- *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires.
- *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset.

config port_security ports

Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the port security:

```
DES-3250:4#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-3250:4#
```

delete port_security_entry vlan_name

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

Example usage:

To delete a port security entry:

```
DES-3250:4#delete port_security_entry vlan_name default
mac_address 00-01-30-10-2C-C7 port 6

Command: delete port_security_entry vlan_name default
mac_address 00-01-30-10-2C-C7 port 6

Success.

DES-3250:4#
```

clear port_security_entry port

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

Example usage:

To clear a port security entry by port:

```
DES-3250:4# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DES-3250:4#
```

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's ports. The information displayed includes port security, admin state, maximum number of learning address and lock mode.
Parameters	*<portlist>* – Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DES-3250:4#show port_security ports 1-5
Command: show port_security ports 1-5

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

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

7

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-3250TG supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

Command	Parameters
create snmp user	<username 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	<usmusername 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_string 32>

Command	Parameters
community	
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 <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> <auth_string 32>
show snmp host	<ipaddr>
create trusted_host	<ipaddr>
delete trusted_host	<ipaddr>
show trusted_host	<ipaddr>
enable snmp traps	
enable snmp authenticate_traps	
show snmp traps	
disable snmp traps	
disable snmp authenticate traps	
config snmp_ system contact	<sw_contact>
config snmp_ system location	<sw_location>
config snmp_ system name	<sw_name>
enable rmon	
disable rmon	

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

create snmp user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.

create snmp user

Syntax	**create snmp user <username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}**
Description	The **create snmp user** command creates a new SNMP user and adds the user to an SNMP group that is also created by this command. SNMP ensures: Message integrity – Ensures that packets have not been tampered with during transit. Authentication – Determines if an SNMP message is from a valid source. Encryption – Scrambles the contents of messages to prevent it from being viewed by an unauthorized source.
Parameters	*<username 32>* – An alphanumeric name of up to 32 characters that will identify the new SNMP user. *<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. *encrypted* – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose: • *by_password* – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the auth_password below. This method is recommended. • *by_key* – Requires the SNMP user to enter a 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 sting of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host. • *<auth_key 32-32>* - Enter an alphanumeric sting of exactly 32 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host. *sha* – Specifies that the HMAC-SHA-96 authentication level will be used.

create snmp user

- *<auth password 8-20>* - An alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.
- *<auth_key 40-40>* - Enter an alphanumeric sting of exactly 40 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host.

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

- *des* – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using:
  - *<priv_password 8-16>* - An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.
  - *<priv_key 32-32>* - Enter an alphanumeric key string of exactly 32 characters, in hex form, that will be used to encrypt the contents of messages the host sends to the agent.
- *none* – Adding this parameter will add no encryption.

Restrictions: Only administrator-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DES-3250:4#create snmp user dlink default encrypted by_password
auth md5 canadian priv none

Command: create snmp user dlink default encrypted by_password
auth md5 canadian priv none


Success.


DES-3250:4#
```

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 <usmusername 32>**
Description	The **delete snmp user** command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	*<usmusername 32>* – An alphanumeric string of up to 32 characters that identifies the SNMP user that will be deleted.

delete snmp user	
	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-3250:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-3250:4#
```

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-3250:4#show snmp user
Command: show snmp user

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

Total Entries: 1

DES-3250:4#
```

create snmp view	
Purpose	Used to assign views to community strings to limit which MIB objects and SNMP manager can access.

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

Example usage:

To create an SNMP view:

```
DES-3250:4#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-3250:4#
```

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

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DES-3250:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-3250:4#
```

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-3250:4#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-3250:4#
```

create snmp

Purpose	Used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The

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

Example usage:

To create the SNMP community string "dlink:"

```
DES-3250:4#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DES-3250:4#
```

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

Example usage:

To delete the SNMP community string "dlink:"

```
DES-3250:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-3250:4#
```

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-3250:4#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-3250:4#
```

config snmp engineID

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

Example usage:

To give the SNMP agent on the Switch the name "0035636666"

```
DES-3250:4#config snmp 0035636666
Command: config snmp engineID 0035636666

Success.

DES-3250:4#
```

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.

show snmp engineID	
	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-3250:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DES-3250:4#
```

create snmp group	
Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	**create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}**
Description	The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	*<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. *v1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity – Ensures that packets have not been tampered with during transit. • Authentication – Determines if an SNMP message is from a

create snmp group

	valid source. • Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. *write_view* – Specifies that the SNMP group being created has write privileges. *notify_view* – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. • *<view_name 32>* – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP group named "sg1:"

```
DES-3250:4#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-3250:4#
```

delete snmp group

Purpose	Used to remove an SNMP group from the Switch.
Syntax	**delete snmp group <groupname 32>**

delete snmp group	
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-3250:4#delete snmp group sg1
Command: delete snmp group sg1

Success.

DES-3250:4#
```

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-3250:4#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-3250:4#
```

create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**create snmp host <ipaddr> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] <auth_string 32>]**
Description	The **create snmp host** command creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipaddr>* – The IP address of the remote management station that will serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity – ensures that packets have not been tampered with during transit. • Authentication – determines if an SNMP message is from a valid source. • Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

create snmp host	
	<auth_sting 32> – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-3250:4#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-3250:4#
```

delete snmp host	
Purpose	Used to remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**delete snmp host <ipaddr> <auth_string 32>**
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. *<auth_sting 32>* – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an SNMP host entry:

```
DES-3250:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DES-3250:4#
```

show snmp host	
Purpose	Used to display the recipient of SNMP traps generated by the Switch's SNMP agent.

show snmp host

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-3250:4#show snmp host
Command: show snmp host

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

Total Entries: 2

DES-3250:4#
```

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-3250:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DES-3250:4#
```

delete trusted_host

Purpose	Used to delete a trusted host entry made using the *create trusted_host* command above.
Syntax	**delete trusted _host <ipaddr>**
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-3250:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DES-3250:4#
```

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-3250:4#show trusted_host
Command: show trusted_host

Management Stations

IP Address
----------------------
10.53.13.94

Total Entries: 1

DES-3250:4#
```

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-3250:4#enable snmp traps
Command: enable snmp traps

Success.

DES-3250:4#
```

enable snmp authenticate traps

Purpose	Used to enable SNMP authentication trap support.
Syntax	**enable snmp authenticate traps**
Description	This command is used to enable SNMP authentication trap support on the Switch.
Parameters	None.

enable snmp authenticate traps

Restrictions	Only administrator-level users can issue this command.

Example Usage:

To turn on SNMP authentication trap support:

```
DES-3250:4#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DES-3250:4#
```

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-3250:4#show snmp traps
Command: show snmp traps

SNMP Traps          : Enabled
Authenticate Traps  : Enabled

DES-3250:4#
```

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.

disable snmp traps	
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To prevent SNMP traps from being sent from the Switch:

```
DES-3250:4#disable snmp traps
Command: disable snmp traps

Success.

DES-3250:4#
```

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

Example Usage:

To disable the SNMP authentication trap support:

```
DES-3250:4#disable snmp authenticate traps
Command: disable snmp authenticate traps

Success.

DES-3250:4#
```

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

config snmp system_contact	
	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-3250:4#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DES-3250:4#
```

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-3250:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3250:4#
```

config snmp system_name	
Purpose	Used to configure the name for the Switch.

config snmp system_name

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-3250TG Switch**":

```
DES-3250:4#config snmp system_name DES-3250TG Switch
Command: config snmp system_name DES-3250TG Switch

Success.

DES-3250:4#
```

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-3250:4#enable rmon
Command: enable rmon

Success.

DES-3250:4#
```

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-3250:4#disable rmon
Command: disable rmon

Success.

DES-3250:4#
```

8

SWITCH UTILITY 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> {all | <unitid 1-8>]} | configuration <ipaddr> <path_filename 64> {increment}]
upload	[configuration | log] <ipaddr> <path_filename 64>
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}

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

download	
Purpose	Used to download and install new firmware or a Switch configuration file from a TFTP server.
Syntax	**download [firmware <ipaddr> <path_filename 64> {unit [all | <unitid 1-8>]} | configuration <ipaddr> <path_filename 64> {increment}]**
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	*firmware* – Download and install new firmware on the Switch from a TFTP server. *configuration* – Download a switch configuration file from a TFTP server. <*ipaddr*> – The IP address of the TFTP server. <*path_filename 64*> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3226S.had. *unit [all* | *<unitid>]* – *all* specifies all units of the switch stack, <*unitid*> is the unit ID of the Switch that will receive the download. *increment* – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only administrator-level users can issue this command.

Example usage:

To download a configuration file:

```
DES-3250:4#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-3250:4#
```

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

Example usage:

To upload a configuration file:

```
DES-3250:4#upload configuration 10.48.74.121 c:\cfg\log.txt
Command: upload configuration 10.48.74.121 c:\cfg\log.txt

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

DES-3250:4#
```

ping	
Purpose	Used to test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}**
Description	The ping command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will

ping	
	then “echo” or return the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters	*<ipaddr>* - Specifies the IP address of the host. *times <value 1-255>* - The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0. *timeout <sec 1-99>* - Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DES-3250:4#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-3250:4#
```

9

NETWORK MONITORING COMMANDS

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

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilitzation	cpu
clear counters	ports <portlist>
clear log	
show log	index <value>
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 <*portlist*>.
Parameters	<*portlist*> – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the packets analysis for port 7 of module 2:

```
DES-3250:4#show packet port 2
```

```
Port number : 2
Frame Size     Frame Counts   Frame/sec     Frame Type     Total     Total/sec
------------   ------------   ----------    ----------     -------   ---------
64             3275           10            RX Bytes       408973    1657
65-127         755            10            RX Frames      395       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 of module 1:

```
DES-3250:4#show error ports 3
Command: show error ports 3

Port number : 1
                RX Frames                      TX Frames
                ---------------                ----------------
CRC Error       19          Excessive Deferral 0
Undersize       0           CRC Error          0
Oversize        0           Late Collision     0
Fragment        0           Excessive Collision 0
Jabber          11          Single Collision   0
Drop Pkts       20837       Collision          0
```

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

show utilization

Purpose	Used to display real-time port and cpu utilization statistics.
Syntax	**show utilization cpu**
Description	This command will display the real-time port and cpu utilization statistics for the Switch.
Parameters	*cpu* – Entering this parameter will display the current cpu utilization of the Switch.
Restrictions	None.

Example usage:

To display the port utilization statistics:

```
DES-3250:4#show utilization
Command: show utilization

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          26         1
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
```

To display the current cpu utilization:

```
DES-3250:4#show utilization cpu

Command: show utilization cpu


CPU utilization :

--------------------------------------------------------------------------------

Five seconds - 15%      One minute - 25%      Five minutes - 14%


DES-3250:4#
```

clear counters

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

Example usage:

To clear the counters:

```
DES-3250:4#clear counters ports 2-9
Command: clear counters ports 2-9


Success.


DES-3250:4#
```

clear log

Purpose	Used to clear the Switch's history log.

clear 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-3250:4#clear log
Command: clear log

Success.

DES-3250:4#
```

show log	
Purpose	Used to display the switch history log.
Syntax	**show log {index <value>}**
Description	This command will display the contents of the Switch's history log.
Parameters	*index* <*value*> – This command will display the history log, beginning at 1 and ending at the value specified by the user in the <*value*> field. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.

Example usage:

To display the switch history log**:**

```
DES-3250:4#show log index 5
Command: show log index 5

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

```
DES-3250:4#
```

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-3250:4#enable syslog
Command: enable syslog

Success.

DES-3250:4#
```

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-3250:4#disable syslog
Command: disable syslog

Success.

DES-3250:4#
```

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-3250:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-3250:4#
```

create syslog host

Purpose	Used to create a new syslog host.
Syntax	**<index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility[local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}**
Description	The **create syslog host** command is used to create a new syslog host.
Parameters	*<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *severity* – Severity level indicator, as shown below: **Bold** font indicates that the corresponding severity level is currently supported on the Switch. Numerical Code — Severity 0 — Emergency: system is unusable 1 — Alert: action must be taken immediately 2 — Critical: critical conditions 3 — Error: error conditions

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.	

create syslog host

Parameters

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 Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon

create 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)**

create syslog host

Parameters	**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

create syslog host	
	remote host. This corresponds to number 23 from the list above. *udp_port <udp_port_number>* – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. *state [enable | disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create syslog host:

```
DES-3250:4#create syslog host 1 severity all facility local0
Command: create syslog host 1 severity all facility local0

Success.

DES-3250:4#
```

config syslog	
Purpose	Used to configure the syslog protocol to send system log data to a remote host.
Syntax	**config syslog {host [all | <index 1-4>]} { severity[informational | warning|all] | facility[local0 | local1 local2 | local3 | local4 | local | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable|diable]}**
Decription	The **config syslog host** command is used to configure the syslog protocol to send system log information to a remote host.
Parameters	*all* – Specifies that the command will be applied to all hosts. *<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.

config syslog

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

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

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	**Warning: warning conditions**
5	Notice: normal but significant condition
6	**Informational: informational messages**
7	Debug: debug-level messages

Parameters

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

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

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

facility – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the"local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font indicates the facility values the Switch currently supports.

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages

config syslog

	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
	8	UUCP subsystem
	9	clock daemon
	10	security/authorization messages
	11	FTP daemon
	12	NTP subsystem
	13	log audit
Parameters	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.

config syslog	
	local3 – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above. *local4* – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above. *local5* – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above. *local6* – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above. *local7* – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above. *udp_port <udp_port_number>* – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. *state [enable | disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure a syslog host:

```
DES-3250:4#config syslog host 1 severity all facility local0
Command: config syslog host all severity all facility ocal0

Success.

DES-3250:4#
```

Example usage:

To configure a syslog host for all hosts:

```
DES-3250:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DES-3250:4#
```

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-3250:4#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3250:4#
```

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-3250:4#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-3250:4#
```

10

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

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

enable stp	
Purpose	Used to globally enable STP on the Switch.
Syntax	**enable stp**
Description	This command allows the Spanning Tree Protocol to be globally enabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DES-3250:4#enable stp
Command: enable stp

Success.

DES-3250:4#
```

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-3250:4#disable stp
Command: disable stp

Success.

DES-3250:4#
```

config stp	
Purpose	Used to setup STP and RSTP on the Switch.
Syntax	{maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30> | priority <value 0-61440> version [rstp | stp] txholdcount <value 1-10> | fbpdu [enable | disable]}
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire Switch. All commands here will be implemented for the STP version that is currently set on the Switch.
Parameters	*maxage <value 6-40>* – This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20. *hellotime <value 1-10>* – The user may set the time interval

config stp	
	between transmission of configuration messages by the root device, thus stating that the Switch is still functioning. A time between 1 and 10 seconds may be chosen, with a default setting of 2 seconds. *forwarddelay* <*value 4-30*> – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds. *priority* <*value 0-61440*> - Select a value between 0 and 61440 to specify the priority for a specified instance ID for forwarding packets. The lower the value, the higher the priority. The port priority value must be divisible by 4094. *Version* [rstp | stp] *A*llows the user to choose the version of the spanning tree to be implemented on the Switch. *txholdcount* <*1-10*> - The maximum number of BDPU Hello packets transmitted per interval. Default value = 3. *fbpdu [enable* | *disable]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *enable*.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DES-3250:4#config stp maxage 18 hellotime 1
Command: config stp maxage 18 hellotime 1

Success.

DES-3250:4#
```

config stp ports	
Purpose	Used to setup STP on the port level.
Syntax	<portlist> {cost [auto | <value 1-200000000>] priority <value 1-240> | migrate [yes | no] | edge [true | false] | p2p [true | false | auto] | state [enable | disable]
Description	This command is used to create and configure STP for a group of ports.
Parameters	*<portlist>* – Specifies a range of ports to be configured. *Cost* – This defines a metric that indicates the relative cost of

config stp ports	
	forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *auto*. • *auto* – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. • <*value 1-200000000*> - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. *priority* <*value 0-240*> - Select a value between 0 and 240 to specify the priority for a specified instance ID for forwarding packets. The lower the value, the higher the priority. The port priority value must be divisible by 16. *migrate [yes | no]* – Setting this parameter as "*yes*" will set the ports to send out BDPU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. *edge [true | false]* – *true* designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status.
Parameters	*p2p [true | false | auto]* – *true* indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were *true*. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *false*. The default setting for this parameter is *auto*. *state [enable | disable]* – Allows STP to be enabled or disabled for the ports specified in the port list. The default is *enable*.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with path cost 19, priority set to 32 seconds, migration enabled, and state enabled for ports 1-5 of module 1.

```
DES-3250:4#config stp ports 1-5 cost 19 priority 32 migrate yes edge true
p2p true state enable

Command: config stp ports 1-5 cost 19 priority 32 migrate yes edge true
```

```
p2p true state enable


Success.

DES-3250:4#
```

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-3250:4#show stp
Command: show stp

STP Status              : Enabled
STP Version             : STP Compatible
Max Age                 : 20
Hello Time              : 2
Forward Delay           : 15
Max Age                 : 20
TX Hold Count           : 3
Forwarding BPDU         : Enabled

DES-3250:4#
```

Status 2 : STP enabled for RSTP

```
DES-3250:4#show stp
Command: show stp

STP Status              : Enabled
```

```
STP Version          : RSTP
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15
Max Age              : 20
TX Hold Count        : 3
Forwarding BPDU      : Enabled

DES-3250:4#
```

show stp ports

Purpose	Used to display the Switch's current spanning tree configuration.
Syntax	**show stp ports <portlist>**
Description	
Parameters	*<portlist>* – Specifies a port or range of ports to be viewed.
Restrictions	None

Example usage:

To show stp ports 1 through 9:

Port	Designated Bridge	State	Cost	Pri	Edge	P2P	Status	Role
1	N/A	Yes	200000	32	No	Yes	Disabled	Disabled
2	N/A	Yes	200000	32	No	Yes	Disabled	Disabled
3	N/A	Yes	200000	32	No	Yes	Disabled	Disabled
4	N/A	Yes	200000	32	No	Yes	Disabled	Disabled
5	N/A	Yes	200000	32	No	Yes	Disabled	Disabled
6	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
7	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
8	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
9	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp
10	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
11	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
12	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
13	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
14	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
15	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
16	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
17	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
18	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
19	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
20	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
21	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp

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

11

FORWARDING DATABASE COMMANDS

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

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

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

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

Example usage:

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

```
DES-3250:4#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DES-3250:4#
```

create multicast_fdb

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

Example usage:

To create multicast MAC forwarding**:**

```
DES-3250:4#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DES-3250:4#
```

config multicast_fdb

Purpose	Used to configure the Switch's multicast MAC address forwarding database.
Syntax	**config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>**
Description	This command configures the multicast MAC address forwarding table.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that will be added to the multicast

config multicast_fdb	
	forwarding table. *[add | delete]* – *add* will add ports to the forwarding table. *delete* will remove ports from the multicast forwarding table. <*portlist*> – Specifies a port or range of ports to be configured.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DES-3250:4#config multicast_fdb default 01-00-00-00-00-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1-1-

Success.

DES-3250:4#
```

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

Example usage:

To set the fdb aging time:

```
DES-3250:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3250:4#
```

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-3250:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3250:4#
```

Example usage:

To delete a multicast fdb entry:

```
DES-3250:4#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DES-3250:4#
```

clear fdb

clear fdb

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

Example usage:

To clear all FDB dynamic entries**:**

```
DES-3250:4#clear fdb all
Command: clear fdb all

Success.

DES-3250:4#
```

show multicast_fdb

Purpose	Used to display the contents of the Switch's multicast forwarding database.
Syntax	**show mulitcast_fdb [vlan <vlan_name 32> | mac_address <macaddr>]**
Description	This command is used to display the current contents of the Switch's multicast MAC address forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that is present in the forwarding database table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DES-3250:4#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

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

Total Entries   : 1

DES-3250:4#
```

show fdb

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

Example usage:

To display unicast MAC address table:

```
DES-3250:4#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID   VLAN Name      MAC Address          Port       Type
```

```
----  ---------------  -----------------  ------  ---------------
1     default          00-00-39-34-66-9A  10      Dynamic
1     default          00-00-51-43-70-00  10      Dynamic
1     default          00-00-5E-00-01-01  10      Dynamic
1     default          00-00-74-60-72-2D  10      Dynamic
1     default          00-00-81-05-00-80  10      Dynamic
1     default          00-00-81-05-02-00  10      Dynamic
1     default          00-00-81-48-70-01  10      Dynamic
1     default          00-00-E2-4F-57-03  10      Dynamic
1     default          00-00-E2-61-53-18  10      Dynamic
1     default          00-00-E2-6B-BC-F6  10      Dynamic
1     default          00-00-E2-7F-6B-53  10      Dynamic
1     default          00-00-E2-82-7D-90  10      Dynamic
1     default          00-00-F8-7C-1C-29  10      Dynamic
1     default          00-01-02-03-04-00  CPU     Self
1     default          00-01-02-03-04-05  10      Dynamic
1     default          00-01-30-10-2C-C7  10      Dynamic
1     default          00-01-30-FA-5F-00  10      Dynamic
1     default          00-02-3F-63-DD-68  10      Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config multicast port_filtering_mode

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

Example usage:

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

```
DES-3250:4#config multicast port_filtering_mode 1-4
forward_all_groups

Command: config multicast port_filtering_mode 1-4
forward_all_groups


Success.
```

```
DES-3250:4#
```

show multicast port_filtering_mode

Purpose	Used to show the multicast packet filtering mode on a port per port basis.
Syntax	**show multicast port_filtering_mode {<portlist>}**
Description	This command will display the current multicast packet filtering mode for specified ports on the Switch.
Parameters	*<portlist>* - Specifies a port or range of ports to view.
Restrictions	None.

Example usage:

To view the multicast port filtering mode for all ports:

```
DES-3250:4#show multicast port_filtering_mode
Command: show multicast port_filtering_mode

Port     Multicast Filter Mode
------   --------------------------
1        forward_unregistered_groups
2        forward_unregistered_groups
3        forward_unregistered_groups
4        forward_unregistered_groups
5        forward_unregistered_groups
6        forward_unregistered_groups
7        forward_unregistered_groups
8        forward_unregistered_groups
9        forward_unregistered_groups
10       forward_unregistered_groups
11       forward_unregistered_groups
12       forward_unregistered_groups
13       forward_unregistered_groups
14       forward_unregistered_groups
15       forward_unregistered_groups
16       forward_unregistered_groups
17       forward_unregistered_groups
18       forward_unregistered_groups
19       forward_unregistered_groups
```

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

12

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_grouplist> | all] { broadcast [enable | disable] | multicast [enable | disable] | dlf [enable | disable] | threshold <value 0-255> }
show traffic control	{group_list <storm_grouplist>}

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

config traffic control

Purpose	Used to configure broadcast/multicast traffic control.
Syntax	**config traffic control [<storm_grouplist> | all] broadcast [enable | disable] | multicast [enable | disable] | dlf [enable | disable] | threshold <value 0-255>**
Description	This command is used to configure broadcast storm control.
Parameters	*<storm_grouplist>* – Used to specify a broadcast storm control group. This is specified by entering the syntax *unit_id*. *all* – Specifies all broadcast storm control groups on the Switch. *broadcast [enable | disable]* – Enables or disables broadcast storm control. *multicast [enable | disable]* – Enables or disables multicast storm control. *dlf [enable | disable]* – Enables or disables dlf traffic control. *threshold <value 0-255>* – The upper threshold at which the specified traffic control is switched on. The <*value*> is the number of broadcast/multicast/dlf packets, in Kbps, received by the Switch that will trigger the storm traffic control measures.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3250:4#config traffic control all broadcast enable
Command: config traffic control all broadcast enable

Success.
```

```
DES-3250:4#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	**show traffic control {group_list <storm_grouplist>}**
Description	This command displays the current storm traffic control configuration on the Switch.
Parameters	*group_list <storm_grouplist>* – Used to specify a broadcast storm control group. This is specified by entering the syntax *unit_id*.
Restrictions	None.

Example usage:

To display traffic control setting:

```
DES-3250:4#show traffic control
Command: show traffic control
Traffic Control

Module  Group [ports]   Threshold   Broadcast Storm   Multicast Storm   Destination Lookup Fail
------  -------------   ---------   ---------         ---------         --------
1       1 [  1-8   ]    128         Disabled          Disabled          Disabled
1       2 [  9-18 ]     128         Disabled          Disabled          Disabled
1       3 [ 17-24]      128         Disabled          Disabled          Disabled
1       4 [    25  ]    128         Disabled          Disabled          Disabled
1       5 [    26  ]    128         Disabled          Disabled          Disabled

Total Entries: 5

DES-3250:4#
```

13

QOS COMMANDS

The DES-3250TG switch supports 802.1p priority queuing. The Switch has 4 priority queues. These priority queues are numbered from 3 (Class 3) — the lowest priority queue — to 0 (Class 0) — the hightest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

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

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the four hardware priority queues in order, beginning with the lowest priority queue, 4, to the highest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

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

Command	Parameters
config bandwidth_control	[<portlist>] {rx_rate [no_limit | <value 1-1000>] | tx_rate [no_limit<value 1-1000>]}
show bandwidth_control	<portlist>
config scheduling	<class_id 0-3> {max_packet <value 0-255> | max_latency <value 0-255>}
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>

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

config bandwidth_control

Purpose	Used to configure bandwidth control on a port by-port basis.
Syntax	**config bandwidth_control [<portlist>] {rx_rate [no_limit | <value 1-1000>] | tx_rate [no_limit<value 1-1000>]}**
Description	The **config bandwidth_control** command is used to configure bandwidth on a port by-port basis.

config bandwidth_control

	bandwidth on a port by-port basis.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *rx_rate* – Specifies that one of the parameters below (*no_limit* or *<value 1-1000>*) will be applied to the rate at which the above specified ports will be allowed to receive packets ▪ *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ *<value 1-1000>* – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive. *tx_rate* – Specifies that one of the parameters below (*no_limit* or *<value 1-1000>*) will be applied to the rate at which the above specified ports will be allowed to transmit packets. ▪ *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ *<value 1-1000>* – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive. The transfer(tx) and receive(rx) rate of packets for Gigabit ports must be configured in a multiple of 8 Mbits. (8, 16, 24…)
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DES-3250:4#config bandwidth_control 1-10 tx_rate 10
Command: config bandwidth_control 1-10 tx_rate 10

Success.

DES-3250:4#
```

show bandwidth_control

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

Example usage:

To display bandwidth control settings:

```
DES-3250:4#show bandwidth_control  1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

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

DES-3250:4#
```

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling <class_id 0-3> [max_packet <value 0-255> | max_latency <value 0-255>]**
Description	The Switch contains 4 hardware priority queues. Incoming packets must be mapped to one of these four queues. This command is used to specify the rotation by which these four hardware priority queues are emptied. The Switch's default (if the config scheduling command is not used, or if the config scheduling command is entered with both max_packet and max_latency parameters are set to 0) is to empty the 4 hardware priority queues in order – from the lowest priority queue (hardware queue 3) to the highest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received. The max_packets parameter allows you to specify the maximum

config scheduling	
	number of packets a given hardware priority queue can transmit before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 255 can be specified. For example, if a value of 3 is specified, then the lowest hardware priority queue (number 3) will be allowed to transmit 3 packets – then the next lowest hardware priority queue (number 2) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat. The max_latency parameter allows you to specify the maximum amount of time that packets are delayed before being transmitted to a given hardware priority queue. A value between 0 and 255 can be specified. This number is then multiplied by 16 ms to determine the maximum latency. For example, if 3 is specified, the maximum latency allowed will be 3 X 16 = 48 ms. When the specified hardware priority queue has been waiting to transmit packets for this amount of time, the current queue will finish transmitting its current packet, and then allow the hardware priority queue whose max_latency timer has expired to begin transmitting packets.
Parameters	*<class_id 0-3>* – This specifies which of the four hardware priority queues the *config scheduling* command will apply to. The four hardware priority queues are identified by number – from 0 to 3 – with the 0 queue being the lowest priority. *max_packet <value 0-255>* – Specifies the maximum number of packets the above specified hardware priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. `A value between 0 and 255 can be specified. *max_latency <value 0-255>* – Specifies the maximum amount of time the above specified hardware priority queue will be allowed to transmit packets before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 255 can be specified – with this value multiplied by 16 ms to arrive at the total allowed time for the queue to transmit packets. For example, a value of 3 specifies 3 X 16 = 48 ms. The queue will continue transmitting the last packet until it is finished when the max_latency timer expires.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each queue:

```
DES-3250:4# config scheduling 0 max_packet 100 max_latency 150
Command: config scheduling 0 max_packet 100 max_latency 150

Success.

DES-3250:4#
```

show scheduling

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

Example usage:

To display the current scheduling configuration:

```
DES-3250:4# show scheduling
Command: show scheduling

QOS Output Scheduling

Class ID     MAX. Packets   MAX. Latency
-----------  -------------- --------------
Class-0      100            150
Class-1      99             100
Class-2      91             101
Class-3      21             201

DES-3250:4#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the four hardware queues available on the Switch.
Syntax	**config 802.1p user_priority <priority 0-7> <class_id 0-3>**
Description	This command allows you to configure the way the Switch will map an incoming packet, based on its 802.1p user priority, to one of the four available hardware priority queues on the Switch. The Switch's default is to map the following incoming 802.1p user priority values to the four hardware priority queues: 802.1p Hardware Queue Remark 0 1 Mid-low

config 802.1p user_priority			
	1	0	Lowest
	2	0	Lowest
	3	1	Mid-low
	4	2	Mid-high
	5	2	Mid-high
	6	3	Highest
	7	3	Highest.
	This mapping scheme is based upon recommendations contained in IEEE 802.1D. You can change this mapping by specifying the 802.1p user priority you want to go to the <*class_id 0-3*> (the number of the hardware queue). <*priority 0-7*> – The 802.1p user priority you want to associate with the <*class_id 0-3*> (the number of the hardware queue) with. <*class_id 0-3*> – The number of the Switch's hardware priority queue. The Switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).		
Restrictions	Only administrator-level users can issue this command.		

Example usage:

To configure 802.1 user priority on the Switch:

```
DES-3250:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-3250:4#
```

show 802.1p user_priority	
Purpose	Used to display the current mapping between an incoming packet's 802.1p priority value and one of the Switch's four hardware priority queues.
Syntax	**show 802.1p user_priority**
Description	The **show 802.1p user_priority** command displays the current mapping of an incoming packet's 802.1p priority value to one of the Switch's four hardware priority queues.

show 802.1p user_priority	
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1p user priority:

```
DES-3250:4# show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

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

DES-3250:4#
```

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

Example usage:

To configure 802.1p default priority on the Switch:

```
DES-3250:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5
```

```
Success.

DES-3250:4#
```

show 802.1 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 configured.
Restrictions	None.

Example usage:

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

```
DES-3250:4# 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
21       0
22       0
23       0
24       0

DES-3250:4#
```

14

PORT MIRRORING COMMANDS

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

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

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

config mirror port

Purpose	Used to configure a mirror port – source port pair on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON proble can then be attached to study the traffic crossing the source port in a completely obtrusive manner.
Syntax	**config mirror port <port> [add | delete] source ports <portlist> [rx | tx | both]**
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	*<port>* – This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be operationg at the same speed a s the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port. *[add | delete]* – Specifies if the user wishes to add or delete ports to be mirrored that are specified in the *source ports* parameter. *source ports* – The port or ports being mirrored. This cannot include the Target port. *<portlist>* – This specifies a port or range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port. *rx* – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list. *tx* – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.

config mirror port	
	both – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	The Target port cannot be listed as a source port. Only administrator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DES-3250:4# config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

DES-3250:4#
```

Example usage:

To delete the mirroring ports:

```
DES-3250:4#config mirror port 1 delete source port 2-4
Command: config mirror 1 delete source 2-4

Success.

DES-3250:4#
```

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	Only administrator-level users can issue this command.

Example usage:

To enable mirroring configurations:

```
DES-3250:4#enable mirror
Command: enable mirror
```

```
Success.

DES-3250:4#
```

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-3250:4#disable mirror
Command: disable mirror

Success.

DES-3250:4#
```

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-3250:4#show mirror
Command: show mirror

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

DES-3250:4#
```

15

VLAN COMMANDS

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

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

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

create vlan

Purpose	Used to create a VLAN on the Switch.
Syntax	**create vlan <vlan_name 32> {tag <vlanid 1-4094> | advertisement}**
Description	This command allows you to create a VLAN on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN to be created. *<vlanid 1-4094>* – The VLAN ID of the VLAN to be created. Allowed values = 1-4094 *advertisement* – Specifies that the VLAN is able to join GVRP. If this parameter is not set, the VLAN cannot be configured to have forbidden ports.
Restrictions	Each VLAN name can be up to 32 characters. If the VLAN is not given a tag, it will be a port-based VLAN. Only administrator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DES-3250:4#create vlan v1 tag 2
Command: create vlan v1 tag 2
```

```
Success.

DES-3250:4#
```

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 you want to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To remove the vlan "v1":

```
DES-3250:4#delete vlan v1
Command: delete vlan v1

Success.

DES-3250:4#
```

config vlan

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}**
Description	This command allows you to add ports to the port list of a previously configured VLAN. You can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	*<vlan_name 32>* – The name of the VLAN you want to add ports to. *add* – Entering the add parameter will add ports to the VLAN. There are three types of ports to add: • *tagged* – Specifies the additional ports as tagged. • *untagged* – Specifies the additional ports as untagged. • *forbidden* – Specifies the additional ports as forbidden *delete* – Deletes ports from the specified VLAN.

config vlan	
	<portlist> – A port or range of ports to add to, or delete from the specified VLAN. *advertisement [enable* | *disable]* – Enables or disables GVRP on the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3250:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DES-3250:4#
```

To delete ports from a VLAN:

```
DES-3250:4#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.

DES-3250:4#
```

config gvrp	
Purpose	Used to configure GVRP on the Switch.
Syntax	**config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}**
Description	This command is used to configure the Group VLAN Registration Protocol on the Switch. You can configure ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).
Parameters	*<portlist>* – A port or range of ports for which you want to enable GVRP for. *all* – Specifies all of the ports on the Switch. *state [enable* | *disable]* – Enables or disables GVRP for the ports specified in the port list. *ingress_checking [enable* | *disable]* – Enables or disables ingress checking for the specified port list.

config gvrp	
	acceptable_frame [tagged_only | *admit_all]* – This parameter states the frame type that will be accepted by the Switch for this function. *tagged_only* implies that only VLAN tagged frames will be accepted, while *admit_all* implies tagged and untagged frames will be accepted byt the Switch. *pvid* <*vlanid 1-4094*> – Specifies the default VLAN associated with the port.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3250:4#config gvrp 1-4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Command: config gvrp 1-4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2


Success.


DES-3250:4#
```

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

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DES-3250:4#enable gvrp

Command: enable gvrp


Success.


DES-3250:4#
```

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

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DES-3250:4#disable gvrp
Command: disable gvrp

Success.

DES-3250:4#
```

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/Forbidden status of each port that is a member of the VLAN.
Parameters	*<vlan_name 32>* – The VLAN name of the VLAN for which you want to display a summary of settings.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DES-3250:4#show vlan
Command: show vlan

VID           : 1          VLAN Name     : default
VLAN TYPE     : static     Advertisement : Enabled
Member ports  : 1,5-26
Static ports  : 1,5-26
```

```
Current Untagged ports   : 1,5-26
Static Untagged ports    : 1,5-26
Forbidden ports   :

VID              : 4094          VLAN Name      : Trinity
VLAN TYPE        : static        Advertisement  : Enabled
Member ports     : 2-4
Static ports     : 2-4
Current Untagged ports   : 2-4
Static Untagged ports    : 2-4
Forbidden ports   :

Total Entries : 2

DES-3250:4#
```

show gvrp

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

Example usage:

To display GVRP port status:

```
DES-3250:4#show gvrp
Command: show gvrp

Global GVRP : Disabled

Port   PVID   GVRP       Ingress Checking  Acceptable Frame Type
------ ----   --------   ----------------  -------------------------
1      1      Disabled   Enabled           All Frames
2      1      Disabled   Enabled           All Frames
3      1      Disabled   Enabled           All Frames
4      1      Disabled   Enabled           All Frames
5      1      Disabled   Enabled           All Frames
6      1      Disabled   Enabled           All Frames
7      1      Disabled   Enabled           All Frames
8      1      Disabled   Enabled           All Frames
9      1      Disabled   Enabled           All Frames
10     1      Disabled   Enabled           All Frames
11     1      Disabled   Enabled           All Frames
```

12	1	Disabled	Enabled	All Frames
13	1	Disabled	Enabled	All Frames
14	1	Disabled	Enabled	All Frames
15	1	Disabled	Enabled	All Frames
16	1	Disabled	Enabled	All Frames
17	1	Disabled	Enabled	All Frames
18	1	Disabled	Enabled	All Frames
19	1	Disabled	Enabled	All Frames
20	1	Disabled	Enabled	All Frames
21	1	Disabled	Enabled	All Frames
22	1	Disabled	Enabled	All Frames
23	1	Disabled	Enabled	All Frames
24	1	Disabled	Enabled	All Frames
25	1	Disabled	Enabled	All Frames
26	1	Disabled	Enabled	All Frames

Total Entries : 24

DES-3250:4#

16

ASYMMETRIC VLAN COMMANDS

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

Command	Parameters
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	

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

enable asymmetric_vlan

Purpose	Used to enable the asymmetric VLAN function on the Switch.
Syntax	**enable asymmetric_vlan**
Description	This command enables the asymmetric VLAN function on the Switch
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable asymmetric VLANs:

```
DES-3250:4#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DES-3250:4#
```

disable asymmetric_vlan

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

Example usage:

To disable asymmetric VLANs:

```
DES-3250:4#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DES-3250:4#
```

show asymmetric_vlan	
Purpose	Used to view the asymmetric VLAN state on the Switch.
Syntax	**show asymmetric_vlan**
Description	This command displays the asymmetric VLAN state on the Switch
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the asymmetric VLAN state cuurently set on the Switch:

```
DES-3250:4#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric Vlan: Enabled

DES-3250:4#
```

17

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <value 1-6> {type [lacp | static]}
delete link_aggregation	group_id <value 1-6>
config link_aggregation	group_id <value1-6> {master_port <port> | ports <portlist> state [enable | disable]}
config link_aggregation algorithm	[mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]
show link_aggregation	{group_id <value 1-6> | algorithm}
config lacp_port	<portlist> mode [active | passive]
show lacp_port	{<portlist>}

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

create link_aggregation

Purpose	Used to create a link aggregation group on the Switch.
Syntax	**create link_aggregation group_id <value 1-6> {type[lacp | static]}**
Description	This command will create a link aggregation group with a unique identifier.
Parameters	*group_id <value>* – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *type* – Specify the type of link aggregation used for the group. If the type is not specified the default type is *static*. • *lacp* – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices. • *static* – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the 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-3250:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DES-3250:4#
```

delete link_aggregation

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

Example usage:

To delete link aggregation group:

```
DES-3250:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DES-3250:4#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-6> {master_port <port> | ports <portlist> | state [enable | disable]**
Description	This command allows you to configure a link aggregation group that was created with the *create link_aggregation* command above. The DES-3250TG supports link_aggregation cross box which specifies that link aggregation groups may be spread over multiple switches in the switching stack.
Parameters	*group _id <value 1-6>* – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.

config link_aggregation

	master_port <port> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. *ports <portlist>* – Specifies a port or range of ports that will belong to the link aggregation group. *state [enable | disable]* – Allows you to enable or disable the specified link aggregation group.
Restrictions	Only administrator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

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

```
DES-3250:4#config link_aggregation group_id 1 master_port 1 ports 5-7, 9
Command: config link_aggregation group_id 1 master_port 1 ports 5-7, 9

Success.

DES-3250:4#
```

config link_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
Syntax	**config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]**
Description	This command configures the part of the packet examined by the Switch when selecting the egress port for transmitting load-sharing data. This feature is only available using the address-based load-sharing algorithm.
Parameters	*mac_source* – Indicates that the Switch should examine the MAC source address. *mac_destination* – Indicates that the Switch should examine the MAC destination address. *mac_source_dest* – Indicates that the Switch should examine the MAC source and destination addresses *ip_source* – Indicates that the Switch should examine the IP source address. *ip_destination* – Indicates that the Switch should examine the IP destination address. *ip_source_dest* – Indicates that the Switch should examine the IP source

config link_aggregation algorithm	
	address and the destination address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3250:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3250:4#
```

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

Example usage:

To display Link Aggregation configuration:

```
DES-3250:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest

Group ID        : 1
Master Port     : 1
Member Port     : 5-10
Active Port     :
Status          : Disabled
```

```
Flooding Port    : 5

DES-3250:4#
```

config lacp_ports

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

Example usage:

To configure LACP port mode settings:

```
DES-3250:4#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DES-3250:4#
```

show lacp_port

Purpose	Used to display current LACP port mode settings.
Syntax	**show lacp_port {<portlist>}**

show lacp_port	
Description	This command will display the LACP mode settings as they are currently configured.
Parameters	<*portlist*> - Specifies a port or range of ports to be configured. If no parameter is specified, the system will display the current LACP status for all ports.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display LACP port mode settings:

```
DES-3250:4#show lacp_port 1-10
Command: show lacp_port 1-10

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

DES-3250:4#
```

18

BASIC IP COMMANDS

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

Command	Parameters
config ipif	<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 <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	*<ipif_name 12>* - Enter an alphanumeric string of up to 12 characters to identify this IP interface. *ipaddress <network_address>* – IP address and netmask of the IP interface to be created. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *<vlan_name 32>* – The name of the VLAN corresponding to the System IP interface. *state [enable | disable]* – Allows you to enable or disable the IP interface. *bootp* – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface. *dhcp* – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DES-3250:4#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DES-3250:4#
```

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>* – The name created for the IP interface.
Restrictions	None.

Example usage:

To display IP interface settings.

```
DES-3250:4#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

Total Entries : 1

DES-3250:4#
```

19

IGMP SNOOPING COMMANDS

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

Command	Parameters
config igmp_snooping	[<vlan_name 32> | all] {host_timeout <sec 1-16711450> | router_timeout < sec 1-16711450> | leave_timer < sec 0-16711450> | state [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 [enable | disable]}
config router_ports	<vlan_name 32> [add | delete] <portlist>
enable igmp_snooping	forward_mcrouter_only
disable igmp_snooping	
show igmp_snooping	vlan <vlan_name 32>
show igmp_snooping group	vlan <vlan_name 32>
show router ports	{vlan <vlan_name 32>} {static | dynamic | forbidden}
show igmp_snooping forwarding	{vlan<vlan_name 32>}
show igmp_snooping group	{vlan<vlan_name 32>}

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]}**
Description	This command allows you to configure IGMP snooping on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping is to be configured. *host_timeout <sec 1-16711450>* – Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. *router_timeout <sec 1-16711450>* – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 260

config igmp_snooping	
	seconds. *leave_timer <sec 1-16711450>* – Specifies the amount of time a Multicast address will stay in the database before it is deleted, after it has sent out a leave group message. An entry of zero (0) specifies an immediate deletion of the Multicast address. The default is 2 seconds. *state [enable | disable]* – Allows you to enable or disable IGMP snooping for the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-3250:4#config igmp_snooping default host_timeout 250 state
enable

Command: config igmp_snooping default host_timeout 250 state
enable


Success.


DES-3250:4#
```

config igmp_snooping querier	
Purpose	This command configures IGMP snooping querier.
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 [enable | disable]**
Description	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.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping querier is to be configured. *query_interval <sec 1-65535>* – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. *max_response_time <sec 1-25>* – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds. *robustness_variable <value 1-255>* – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness

config igmp_snooping querier

	variable is used in calculating the following IGMP message intervals: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy. Although 1 is specified as a valid entry, the roubustness variable should not be one or problems may arise. *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. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. *state [enable*	*disable]* – Allows the Switch to be specified as an IGMP Querier or Non-querier.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-3250:4#config igmp_snooping querier default query_interval 125
state enable

Command: config igmp_snooping querier default query_interval 125
state enable


Success.


DES-3250:4#
```

config router_ports

Purpose	Used to configure ports as router ports.
Syntax	**config router_ports <vlan_name 32> [add | delete] <portlist>**

config router_ports	
Description	This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *<portlist>* – Specifies a port or range of ports that will be configured as router ports.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set up static router ports:

```
DES-3250:4#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DES-3250:4#
```

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

Example usage:

To enable IGMP snooping on the Switch:

```
DES-3250:4#enable igmp_snooping
Command: enable igmp_snooping

Success.
```

```
DES-3250:4#
```

disable igmp_snooping

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

Example usage:

To disable IGMP snooping on the Switch:

```
DES-3250:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3250:4#
```

Example usage:

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

```
DES-3250:4#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only

Success.

DES-3250:4#
```

show igmp_snooping

Purpose	Used to show the current status of IGMP snooping on the Switch.

show igmp_snooping

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 to view the IGMP snooping configuration for.
Restrictions	None.

Example usage:

To show IGMP snooping:

```
DES-3250:4#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

VLAN  Name                    : vlan2
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


Total Entries: 2

DES-3250:4#
```

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>}**

show igmp_snooping group	
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-3250:4#show igmp_snooping group
Command: show igmp_snooping group

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

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

VLAN Name      : default
Multicast group: 234.5.6.7
MAC address    : 01-00-5E-05-06-07
Reports        : 1
Port Member    : 4,10

VLAN Name      : default
Multicast group: 236.54.63.75
MAC address    : 01-00-5E-36-3F-4B
Reports        : 1
Port Member    : 18,22

VLAN Name      : default
Multicast group: 239.255.255.250
MAC address    : 01-00-5E-7F-FF-FA
Reports        : 2
Port Member    : 9,19

VLAN Name      : default
Multicast group: 239.255.255.254
MAC address    : 01-00-5E-7F-FF-FE
```

```
Reports          : 1
Port Member      : 13,17

Total Entries    : 6

DES-3250:4#
```

show router_ports

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

Example usage:

To display the router ports.

```
DES-3250:4#show router_ports
Command: show router_ports

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

Total Entries: 1

DES-3250:4#
```

show igmp_snooping forwarding

Purpose	Used to display the IGMP snooping forwarding table entries on the Switch.
Syntax	**show igmp_snooping forwarding {vlan <vlan_name 32>}**
Description	This command will display the current IGMP snooping forwarding table entries currently configured on the Switch.

show igmp_snooping forwarding	
Parameters	<*vlan_name 32*> – The name of the VLAN for which to view IGMP snooping forwarding table information.
Restrictions	None.

Example usage:

To view the IGMP snooping forwarding table for VLAN "Trinity":

```
DES-3250:4#show igmp_snooping forwarding vlan Trinity
Command: show igmp_snooping forwarding vlan Trinity

VLAN Name      : Trinity
Multicast group : 224.0.0.2
MAC address    : 01-00-5E-00-00-02
Port Member    : 17

Total Entries: 1

DES-3250:4#
```

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

Example usage:

To view the current IGMP snooping group:

```
DES-3250:4#show igmp_snooping group
Command: show igmp_snooping group

VLAN Name      : default
Multicast group : 224.0.0.2
MAC address    : 01-00-5E-00-00-02
Reports        : 1
```

```
Port Member         : 2,4

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

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

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

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

Total Entries : 6

DES-3250:4#
```

20

802.1X COMMANDS

The DES-3250TG implements the server-side of the IEEE 802.1x Port-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	
show 802.1x auth_configuration	{ports <portlist>}
show 802.1x auth_state	{ports <portlist>}
config 802.1x capability ports	[<portlist> | all] [authenticator | none]
config 802.1x auth_parameter ports	[<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]
config 802.1x init	{port_based ports [<portlist> | all] | mac_based [ports] [<portlist> |all] {mac_address <macaddr>}]
config 802.1x auth_mode	[port_based | mac_based]
config 802.1x reauth	{port_based ports [<portlist> | all] | mac_based [ports] [<portlist> |all] {mac_address <macaddr>}]
config radius add	<server_index 1-3> <server_ip> key <passwd 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}]
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> {ipaddress <server_ip> | key <passwd 32> [auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>]}
show radius	

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

enable 802.1x

Purpose	Used to enable the 802.1x server on the Switch.
Syntax	**enable 802.1x**
Description	The *enable 802.1x* command enables the 802.1x Port-based Network Access control server application on the Switch.
Parameters	None.

enable 802.1x	
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable 802.1x switch wide:

```
DES-3250:4#enable 802.1x
Command: enable 802.1x

Success.

DES-3250:4#
```

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 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-3250:4#disable 802.1x
Command: disable 802.1x

Success.

DES-3250:4#
```

show 802.1x auth_configuration	
Purpose	Used to display the current configuration of the 802.1x server on the Switch.
Syntax	**show 802.1x auth_configuration {ports <portlist>}**
Description	The show 802.1x command is used to display the current configuration of the 802.1x Port-based Network Access Control server application on the Switch.
Parameters	*ports* <*portlist*> – Specifies a port or range of ports to view.

show 802.1x auth_configuration

	The following details are displayed: 802.1x Enabled / Disabled – Shows the current status of 802.1x functions on the Switch. Authentication Mode – Shows the authentication mode, whether it be by MAC address or by port. Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the Switch and a RADIUS server. May read *Radius_Eap* or *Radius_Pap.* Port number – Shows the physical port number on the Switch. Capability: Authenticator|None – Shows the capability of 802.1x functions on the port number displayed above. There are two 802.1x capabilities that can be set on the Switch: Authenticator and None. AdminCtlDir: Both / In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. OpenCtlDir: Both / In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. Port Control: ForceAuth / ForceUnauth / Auto – Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized. QuietPeriod – 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 / Identiy 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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x authtication states:

```
DES-3250:4#show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

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

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

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

show 802.1x auth_state

Purpose	Used to display the current authentication state of the 802.1x server on the Switch.
Syntax	**show 802.1x auth_state {ports <portlist>}**
Description	The show 802.1x auth_state command is used to display the current authentication state of the 802.1x Port-based Network Access Control server application on the Switch.
Parameters	*ports <portlist>* – Specifies a port or range of ports to be viewed. The following details what is displayed: Port number – Shows the physical port number on the Switch. Auth PAE State: Initalize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE. Backend State: Request / Response / Fail / Idle / Initalize / Success / Timeout – Shows the current state of the Backend Authenticator.

show 802.1x auth_state

	Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x auth state:

```
DES-3250:4#show 802.1x auth_state
Command: show 802.1x auth_state

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

config 802.1x capability ports

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

Example usage:

To configure 802.1x capability on ports 1-10:

```
DES-3250:4#config 802.1x capability ports 1 – 10 authenticator
Command: config 802.1x capability ports 1 – 10 authenticator

Success.

DES-3250:4#
```

config 802.1x auth_parameter ports

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

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

Example usage:

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

```
DES-3250:4#config 802.1x auth_parameter ports 1–20 direction both
Command: config 802.1x auth_parameter ports 1–20 direction both
```

```
Success.

DES-3250:4#
```

config 802.1x init

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

Example usage:

To initialize the authentication state machine of all ports:

```
DES-3250:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-3250:4#
```

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.

config 802.1x auth_mode	
Parameters	*[port_based* | *mac_based]* – The Switch allows you to authenticate 802.1x by either port or MAC address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication by MAC address:

```
DES-3250:4#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DES-3250:4#
```

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 port number.
Parameters	*port_based* – This instructs the Switch to re-authorize 802.1x functions based only on the port number. Ports approved for re-authorization can then be specified. *mac_based* – This instructs the Switch to re-authorize 802.1x functions based only on the MAC address. MAC addresses approved for re-authorization can then be specified. *ports* <*portlist*> – Specifies a port or range of ports to be re-authorized. *all* – Specifies all of the ports on the Switch. *mac_address* <*macaddr*> - Enter the MAC address to be re-authorized.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-18:

```
DES-3250:4#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18
```

```
Success.

DES-3250:4#
```

config radius add

Purpose	Used to configure the settings the Switch will use to communicate with a RADIUS server.
Syntax	**config radius add <server_index 1-3> <server_ip> key <passwd 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}]**
Description	The **config radius add** command is used to configure the settings the Switch will use to communicate with a RADIUS server.
Parameters	*<server_index 1-3>* – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the Switch. *<server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key will be used between the Switch and the Radius server. *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. *default* – Uses the default udp port number in both the "auth_port" and "acct_port" settings. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is 1813.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the RADIUS server communication setttings:

```
DES-3250:4#config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DES-3250:4#
```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.

config radius delete

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

Example usage:

To delete previously configured RADIUS server communication settings:

```
DES-3250:4#config radius delete 1
Command: config radius delete 1

Success.

DES-3250:4#
```

config radius

Purpose	Used to configure the Switch's RADIUS settings.
Syntax	**config radius <server_index 1-3> {ipaddress <server_ip> | key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}**
Description	The **config radius** command is used to configure the Switch's Radius settings.
Parameters	*<server_index 1-3>* – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the Switch. *ipaddress <server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key will be used between the Switch and the RADIUS server. • *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is 1813.

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

Example usage:

To configure the RADIUS settings:

```
DES-3250:4#config radius 1 10.48.74.121 key dlink default
Command: config radius 1 10.48.74.121 key dlink default

Success.

DES-3250:4#
```

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-3250:4#show radius
Command: show radius

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

Total Entries : 3

DES-3250:4#
```

21

ACCESS CONTROL LIST (ACL) COMMANDS

The DES-3250TG implements Access Control Lists that enable the Switch to deny network access to specific devices or device groups based on IP settings or MAC address.

Command	Parameters
create access_profile	[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code } | igmp {type } | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>| flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-xffff>} | protocol_id_mask <hex0x0 - 0xFF> {user_define_mask <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] {port [<portlist> | all] | profile_id <value 1-255>}
delete access_profile	<value 1-255>
config access_profile profile_id	<value 1-255> [add access_id <value 1-255> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] [permit {priority <value 0-7> {replace_priority} | replace_dscp_with <value 0-63> } | deny] | delete access_id <value 1-255>]
show access_profile	{profile_id <value 1-255>}

Due to a chipset limitation, the Switch currently supports a maximum of 9 access profiles, each containing a maximum of 50 rules – with the additional limitation of 50 rules total for all 9 access profiles.

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

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

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1

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

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

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

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 deny

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

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

create access_profile

Purpose	Used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code } | igmp {type } | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>| flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-xffff>} | protocol_id_mask <hex0x0 - 0xFF> {user_define_mask <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] {port [<portlist> | all] | profile_id <value 1-255>}**
Description	The **create access_profile** command is used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that

create access_profile

will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.

Parameters

ethernet – Specifies that the Switch will examine the layer 2 part of each packet header.

- *vlan* – Specifies that the Switch will examine the VLAN part of each packet header.
- *source_mac <macmask>* – Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format.
- *destination_mac <macmask>* – Specifies a MAC address mask for the destination MAC address.
- *802.1p* – Specifies that the Switch will examine the 802.1p priority value in the frame's header.
- *ethernet_type* – Specifies that the Switch will examine the Ethernet type value in each frame's header.

ip – Specifies that the Switch will examine the IP address in each frame's header.

- *vlan* – Specifies a VLAN mask.
- *source_ip_mask <netmask>* – Specifies an IP address mask for the source IP address.
- *destination_ip_mask <netmask>* – Specifies an IP address mask for the destination IP address.
- *dscp* – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.
- *icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.
  - *type* – Specifies that the Switch will examine each frame's ICMP Type field.
  - *code* – Specifies that the Switch will examine each frame's ICMP Code field.
- *igmp* – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.
  - *type* – Specifies that the Switch will examine each frame's IGMP Type field.
- *tcp* – Specifies that the Switch will examine each frames Transport Control Protocol (TCP) field.

Parameters

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

create access_profile

	• *dst_port_mask* <*hex 0x0-0xffff*> – Specifies a TCP port mask for the destination port. • *flag_mask [all* | *{urg* | *ack* | *psh* | *rst* | *syn* | *fin}]* – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits asscociated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between *all, urg* (urgent), *ack* (acknowledgement), *psh* (push), *rst* (reset), *syn* (synchronize) and *fin* (finish). • *udp* – Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field. • *src_port_mask* <*hex 0x0-0xffff*> – Specifies a UDP port mask for the source port. • *dst_port_mask* <*hex 0x0-0xffff*> – Specifies a UDP port mask for the destination port. • *protocol_id* – Specifies that the Switch will examine each frame's Protocol ID field. • *user_define_mask* <*hex 0x0-0xffffffff*> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header. • *packet_content_mask* – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-15* – Enter a value in hex form to mask the packet from the beginning of the packet to the 16th byte. • *offset_16-31* – Enter a value in hex form to mask the packet from byte 16 to byte 31. • *offset_32-47* – Enter a value in hex form to mask the packet from byte 32 to byte 47. • *offset_48-63* – Enter a value in hex form to mask the packet from byte 48 to byte 63. • *offset_64-79* – Enter a value in hex form to mask the packet from byte 64 to byte 79.
Parameters	*port* <*portlist*> - Specifies a port or range of ports to be configured. *all* – Denotes all ports on the Switch. *profile_id* <*value 1-255*> – Specifies an index number that will identify the access profile being created with this command.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an access list rules:

```
DES-3250:4#create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code permit profile_id 101

Command: create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code permit profile_id 101


Success.


DES-3250:4#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile [profile_id <value 1-255>]**
Description	The **delete access_profile** command is used to delete a previously created access profile on the Switch.
Parameters	*profile_id <value 1-255>* – Enter an integer between 1 and 255 that is used to identify the access profile that will be deleted with this command. This value is assigned to the access profile when it is created with the **create access_profile** command.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3250:4# delete access_profile profile_id 1

Command: delete access_profile profile_id 1


Success.


DES-3250:4#
```

config access_profile profile_ID

Purpose	Used to configure an access profile on the Switch and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using

config access_profile profile_ID

	the **create access_profile** command will be combined, using a logical AND operation, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**<value 1-255>[add access_id <value 1-255> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] [permit {priority <value 0-7> {replace_priority} | replace_dscp_with <value 0-63> } | deny] | delete access_id <value 1-255>]**
Description	The **config access_profile** command is used to configure an access profile on the Switch and to enter specific values that will be combined, using a logical AND operation, with masks entered with the **create access_profile** command, above.
Parameters	*profile_id <value 1-255>* – Enter an integer between 1 and 8 that is used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the *create access_profile* command. *add access_id <value 1-255>* – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. The lower access ID, the higher the priority the rule will be given. *ethernet* – Specifies that the Switch will look only into the layer 2 part of each packet. • *vlan <vlan_name 32>* – Specifies that the access profile will apply to only to this VLAN. • *source_mac <macaddr>* – Specifies that the access profile will apply to only packets with this source MAC address.
Parameters	• *destination_mac <macaddr>* – Specifies that the access profile will apply to only packets with this destination MAC address. • *802.1p <value 0-7>* – Specifies that the access profile will apply only to packets with this 802.1p priority value.

config access_profile profile_ID

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

ip – Specifies that the Switch will look into the IP fields in each packet.

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only this VLAN.
- *source_ip <ipaddr>* – Specifies that the access profile will apply to only packets with this source IP address.
- *destination_id <value 0-255>* – Specifies that the access profile will apply to only packets with this destination IP address.
- *dscp <value 0-63>* – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.
- *priority <value 0-7>* – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header.
- *dscp <value 0-63>* – Allows you to specify a value to be written to the DSCP field of an incoming packet.
- *icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.
  - *type <value 0-65535>* – Specifies that the access profile will apply to this ICMP type value.
  - *code <value 0-255>* – Specifies that the access profile will apply to this ICMP code.
- *igmp* – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.
  - *type <value 0-255>* – Specifies that the access profile will apply to packets that have this IGMP type value.
- *tcp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.
  - *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.
  - *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.
- *flag_mask* – Enter the type of TCP flag to be masked. The choices are:

config access_profile profile_ID

- *all*: all flags are selected.
- *urg*: TCP control flag (urgent)
- *ack*: TCP control flag (acknowledgement)
- *psh*: TCP control flag (push)
- *rst*: TCP control flag (reset)
- *syn*: TCP control flag (synchronize)
- *fin*: TCP control flag (finish)

- *udp* – Specifies that the Switch will examine the Universal Datagram Protocol (UDP) field in each packet.
  - *src_port* <*value 0-65535*> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.
  - *dst_port* <*value 0-65535*> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.
- *protocol_id* <*value 0-255*> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.
- *user_define* <*hex 0x0-0xffffffff*> – Specifies a mask to be combined with the value found in the frame header using a logical AND operation.
- *packet_content_mask* – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows:
  - *offset_0-15* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte.
  - *offset_16-31* - Enter a value in hex form to mask the packet from byte 16 to byte 32.
  - offset_32-47 - Enter a value in hex form to mask the packet from byte 32 to byte 47.
  - *offset_48-63* - Enter a value in hex form to mask the packet from byte 48 to byte 63.
- *offset_64-79* - Enter a value in hex form to mask the packet from byte 64 to byte 79.

permit – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

- *priority* <*value 0-7*> – Specify the 802.1p priority value included in the packet that will be forwarded by the Switch. Only

config access_profile profile_ID	
	packets that have this priority value will be permitted. • *{replace_priority}* – This parameter is specified if you want to change the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being transmitted from the Switch. *replace_dscp with <value 0-63>* – Allows you to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet. *deny* – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered. *delete access_id <value 1-255>* – Specifies the access ID of a rule to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the access profile with the profile ID of 1 to filter frames that have IP addresses in the range between 10.42.73.0 to 10.42.73.255:

```
DES-3250:4# config access_profile profile_id 2 add access_id 1 ip
source_ip 10.42.73.1 deny

Command: config access_profile profile_id 1 add access_id 1 ip
source_ip 10.42.73.1 deny


Success.


DES-3250:4#
```

show access_profile

Purpose	Used to display the currently configured access profiles on the Switch.
Syntax	**show access_profile**
Description	The **show access_profile** command is used to display the currently configured access profiles.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3250:4#show access_profile
Command: show access_profile


Access Profile Table


Access Profile ID : 4
Type    : IP Frame Filter
Ports   : All
Masks   : VLAN
        ----------------


ID   Mode
---  ------    ----------------
1   Permit  default


Access Profile ID : 246
```

```
Type      : IP Frame Filter
Ports     : All
Masks     : Source IP Addr
          ---------------
          255.0.0.0
ID  Mode
---  ------   ---------------

Access Profile ID : 247
Type      : Ethernet Frame Filter
Ports     : All
Masks     : 802.1p
          ------

ID  Mode
---  ------ ------

Access Profile ID : 249
Type      : Packet Content Filter
Ports     : All
Masks     : Offset 0-15  : 0x00000000 00000000 00000000 00000000
          Offset 16-31 : 0x00000000 00000000 00000000 00000000
          Offset 32-47 : 0x00000000 00000000 00000000 00000000
          Offset 48-63 : 0x00000000 00000000 00000000 00000000
          Offset 64-79 : 0x00000000 00000000 00000000 00000000

DES-3250:4#
```

22

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.

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

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

config traffic_segmentation

Purpose	Used to configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation [<portlist>] forward_list [null | <portlist>]**
Description	The **config traffic_segmentation** command is used to configure traffic segmentation on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports that will be configured for traffic segmentation. *forward_list* – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above. • *null* – No ports are specified • *<portlist>* – Specifies a range of ports for the forwarding list. This list must be on the same Switch previously specified for traffic segmentation (i.e. following the *<portlist>* specified above for config traffic_segmentation).
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure ports 1 through 10 to be able to forward frames to port 11 through 15:

```
DES-3250:4# config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DES-3250:4#
```

show traffic_segmentation	
Purpose	Used to display the current traffic segmentation configuration on the Switch.
Syntax	**show traffic_segmentation <portlist>**
Description	The **show traffic_segmentation** command is used to display the current traffic segmentation configuration on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports for which the current traffic segmentation configuration on the Switch will be displayed.
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-3250:4#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

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

23

STACKING COMMANDS

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

Command	Parameters
config stacking mode	[disable | enable [master | auto | slave]]
show stacking	{mode}

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

NOTE: The default settings for the switch allow the switch to function as either a member of a stacked group or as a standalone device.

config stacking mode

Purpose	Used to enable or disable switch stacking and to configure the stacking mode.
Syntax	**config stacking mode [disable | enable [auto | slave]]**
Description	Use this command to setup switch stacking or disable the stacking function. Each switch should be configured separately prior to establishing the physical link through the stacking ports.
Parameters	enable – Stacking mode is enabled by default. When enabled the switch can operate as a standalone device or it can be allowed to operate with other DES 3250 switches in a stacked group. disable – This forces the switch to operate as a standalone device. In standalone mode the switch functions as a standalone device even if a stacking module is installed. When stacking mode is disabled, configuration settings including IP settings are saved in an alternate configuration file. A switch that has stacking mode disabled should not use stacking ports if they are present. auto – This is the default stacking mode setting for the switch. In auto stacking mode the switch is eligible for stacking or it can operate as a standalone device. If a switch stack is connected and all switches are configured to operates in auto stacking mode, the master-slave relationships and stacking order will be determined automatically according to MAC address. The lowest MAC address becomes the master (stack number 1). The order in which slave devices appear logically in the stack (stack

config stacking mode	
	number 2+) is determined by how they are connected relative to the master switch. The auto mode serves to first determine if the device is stacked or standalone, then if stacked, it determines which switch is the master and the remaining stack numbers for the slave switches. slave – This overrides the auto stacking mode. When the switch is in slave mode in cannot function as a master and a master switch must be properly connected to the stack for a switch to operate in slave mode.
Restrictions	The switch's stacking mode can only be changed using the CLI interface. Only administrator-level users can issue this command.

Example usage:

To configure the stacking mode:

```
DES-3250:4#config stacking mode disable
Command: config stacking mode disable

Do you want to save the system's configuration to NV-RAM?(y/n)
Saving all configurations to NV-RAM... Done.
Success.

DES-3250:4#
```

show stacking	
Purpose	Used to display the current stacking information.
Syntax	**show stacking {mode}**
Description	This command will display the current stacking information.
Parameters	mode – When specified this will display the current stacking mode. {mode} – No specification will display information for all switches in the stack. Information displayed includes MAC address, firmware version, stacking mode, RPS status and available port range.
Restrictions	None.

Example usage:

To display the current stacking information:

```
DES-3250:4#show stacking
Command: show stacking

ID   MAC Address         Port Range  Mode       Version     RPS Status   Model
Name
---  ----------------    ----------  ---------- --------    ----------   ----------
*1   00-01-02-03-04-00   1 - 50      AUTO       4.00-B11    Not Support  DES-3250

Total Entries :1
DES-3250:4#
```

Example usage:

To display stacking mode:

```
DES-3250:4#show stacking mode
Command: show stacking mode

Setting         : AUTO
Current         : STANDALONE

DES-3250:4#
```

24

TIME AND SNTP COMMANDS

The Simple Network Time Protocol (SNTP) (an adaptation of the Network Time Protocol (NPT)) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config sntp	{primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	<date ddmmmyyyy > <time hh:mm:ss >
config time_zone	{operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst	[disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat>| s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e-day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]
show time	

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

config sntp

Purpose	Used to setup SNTP service.
Syntax	**config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}**
Description	Use this command to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See *enable sntp*).
Parameters	*primary* – This is the primary server the SNTP information will be taken from. • <*ipaddr*> – The IP address of the primary server. *secondary* – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable. • <*ipaddr*> – The IP address for the secondary server. *poll-interval <int 30-99999>* – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.

config sntp	
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-3250:4#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-3250:4#
```

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-3250:4#show sntp
Command: show sntp


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


DES-3250:4#
```

enable sntp	
Purpose	To enable SNTP server support.

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

Example usage:

To enable the SNTP function:

```
DES-3250:4#enable sntp
Command: enable sntp

Success.

DES-3250:4#
```

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

Example:

To disable SNTP support:

```
DES-3250:4#disable sntp
Command: disable sntp

Success.

DES-3250:4#
```

config time	
Purpose	Used to manually configure system time and date settings.

config time

Syntax	**config time <date ddmmmyyyy> <time hh:mm:ss>**
Description	This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	*date* – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003. *time* – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.
Restrictions	Only administrator-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
DES-3250:4#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3250:4#
```

config time_zone

Purpose	Used to determine the time zone used in order to adjust the system clock.
Syntax	**config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}**
Description	This will adjust system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	*operator* – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT. *hour* – Select the number of hours different from GMT. *min* – Select the number of minutes difference added or subtracted to adjust the time zone.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DES-3250:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3250:4#
```

config dst

Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	**config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]**
Description	DST can be enabled and configured using this command. When enabled this will adjust the system clock to comply with any DST requirement. DST adjustment effects system time for both manually configured time and time set using SNTP service.
Parameters	*disable* - Disable the DST seasonal time adjustment for the Switch. *repeating* - Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October. *annual* - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. *s_week* - Configure the week of the month in which DST begins. • *<start_week 1-4,last>* - The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *e_week* - Configure the week of the month in which DST ends. • *<end_week 1-4,last>* - The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *s_day* – Configure the day of the week in which DST begins.

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

Example usage:

To configure daylight savings time on the Switch:

```
DES-3250:4#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-3250:4#
```

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 cuurently set on the Switch's System clock:

```
DES-3250:4#show time
Command: show time

Current Time Source : System Clock
Boot Time           : 0 Days 00:00:00
Current Time        : 1 Days 01:39:17
Time Zone           : GMT +02:30
Daylight Saving Time : Repeating
Offset in Minutes   : 30
  Repeating From    : Apr 2nd Tue 15:00
            To      : Oct 2nd Wed 15:30
  Annual    From    : 29 Apr 00:00
            To      : 12 Oct 00:00


DES-3250:4#
```

25

ARP COMMANDS

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

Command	Parameters
create arpentry	<ipaddr> <macaddr>
config arpentry	<ipaddr> <macaddr>
delete arpentry	{[<ipaddr> | all]}
show arpentry	{ipif <ipif_name 12> | ipaddress <ipaddr> | [static | local]}
config arp_aging time	<value 0-65535>
clear arptable	

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

create arpentry

Purpose	Used to make a static entry into the ARP table.
Syntax	**create arpentry <ipaddr> <macaddr>**
Description	This command is used to enter an IP address and the corresponding MAC address into the Switch's ARP table.
Parameters	*<ipaddr>* – The IP address of the end node or station. *<macaddr>* – The MAC address corresponding to the IP address above.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create a static arp entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
DES-3250:4#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

 Success.

DES-3250:4#
```

config arpentry

Purpose	Used to configure a static entry in the ARP table.
Syntax	**config arpentry <ipaddr> <macaddr>**

config arpentry

Description	This command is used to configure a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the Switch's ARP table.
Parameters	<*ipaddr*> – The IP address of the end node or station. <*macaddr*> – The MAC address corresponding to the IP address above.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure a static arp entry for the IP address 10.48.74.12 and MAC address 00:50:BA:00:07:36:

```
DES-3250:4#config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

Success.

DES-3250:4#
```

delete arpentry

Purpose	Used to delete a static entry into the ARP table.
Syntax	**delete arpentry {[<ipaddr> | all]}**
Description	This command is used to delete a static ARP entry, made using the *create arpentry* command above, by specifying either the IP address of the entry or all. Specifying *all* clears the Switch's ARP table.
Parameters	<*ipaddr*> – The IP address of the end node or station. *all* – Deletes all ARP entries.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DES-3250:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-3250:4#
```

config arp_aging time

Purpose	Used to configure the age-out timer for ARP table entries on the Switch.
Syntax	**config arp_aging time <value 0-65535>**
Description	This command sets the maximum amount of time, in minutes, that an ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	*time <value 0-65535>* – The ARP age-out time, in minutes. The value may be set in the range of 0-65535 minutes with a default setting of 20 minutes.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```
DES-3250:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3250:4#
```

show arpentry

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

Example Usage:

To display the ARP table**:**

```
DES-3250:4#show arpentry
Command: show arpentry

 ARP Aging Time : 30

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-3250:4#
```

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-3250:4#clear arptable
Command: clear arptable

Success.

DES-3250:4#
```

26

ROUTING TABLE COMMANDS

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

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

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

create iproute

Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	**create iproute [default] <ipaddr> {<metric 1-65535>}**
Description	This command is used to create a default static IP route entry to the Switch's IP routing table.
Parameters	*<ipaddr>* – The gateway IP address for the next hop router. *<metric 1-65535>* – Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add the default static address 10.48.74.121, with a metric setting of 1, to the routing table:

```
DES-3250:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DES-3250:4#
```

delete iproute

Purpose	Used to delete a default IP route entry from the Switch's IP routing table.
Syntax	**delete iproute [default]**
Description	This command will delete an existing default entry from the Switch's IP routing table.

delete iproute

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

Example usage:

To delete the default IP route 10.53.13.254:

```
DES-3250:4#delete iproute default 10.53.13.254
Command: delete iproute default 10.53.13.254

Success.

DES-3250:4#
```

show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	**show iproute {network_address> } {static}**
Description	This command will display the Switch's current IP routing table.
Parameters	<network_address> – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Example Usage:

To display the contents of the IP routing table:

```
DES-3250:4#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-3250:4#
```

27

MAC NOTIFICATION COMMANDS

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

Command	Parameters
enable mac_notification	
disable mac_notification	
config mac_notification	{interval <int 1-2147483647> | historysize <int 1-500>
config mac_notification ports	[<portlist> | all] [enable | disable]
show mac_notification	
show mac_notification ports	<portlist>

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

enable mac_notification

Purpose	Used to enable global MAC address table notification on the Switch.
Syntax	**enable mac_notification**
Description	This command is used to enable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable MAC notification without changing basic configuration:

```
DES-3250:4#enable mac_notification
Command: enable mac_notification

Success.

DES-3250:4#
```

disable mac_notification

Purpose	Used to disable global MAC address table notification on the Switch.
Syntax	**disable mac_notification**

disable mac_notification

Description	This command is used to disable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable MAC notification without changing basic configuration:

```
DES-3250:4#disable mac_notification
Command: disable mac_notification

Success.

DES-3250:4#
```

config mac_notification

Purpose	Used to configure MAC address notification.
Syntax	**config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>**
Description	MAC address notificiation is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*interval <sec 1-2147483647>* - The time in seconds between notifications. The user may choose an interval between 1 and 2,147,483,647 seconds. *historysize <1 - 500>* - The maximum number of entries listed in the history log used for notification.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the Switch's MAC address table notification global settings:

```
DES-3250:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DES-3250:4#
```

config mac_notification ports	
Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist | all] [enable | disable]**
Description	MAC address notificiation is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist>* - Specify a port or range of ports to be configured. *all* – Entering this command will set all ports on the system. *[enable | disable]* – These commands will enable or disable MAC address table notification on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DES-3250:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-3250:4#
```

show mac_notification	
Purpose	Used to display the Switch's MAC address table notification global settings
Syntax	**show mac_notification**
Description	This command is used to display the Switch's MAC address table notification global settings.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To view the Switch's MAC address table notification global settings:

```
DES-3250:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State          : Enabled
Interval       : 1
History Size   : 1

DES-3250:4#
```

show mac_notification ports

Purpose	Used to display the Switch's MAC address table notification status settings
Syntax	**show mac_notification ports <portlist>**
Description	This command is used to display the Switch's MAC address table notification status settings.
Parameters	*<portlist>* - Specify a port or group of ports to be viewed. Entering this command without the parameter will display the MAC notification table for all ports.
Restrictions	None

Example usage:

To display all port's MAC address table notification status settings:

```
DES-3250:4#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------  ------------------------------------------------------
1                   Disabled
2                   Disabled
3                   Disabled
4                   Disabled
5                   Disabled
6                   Disabled
7                   Disabled
8                   Disabled
```

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

28

COMMAND HISTORY LIST

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

Command	Parameters
?	
dir	
config command_history	<value 1-40>
show command_history	
clear	

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

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	?
Description	This command will display all of the commands available through the Command Line Interface (CLI).
Parameters	None.
Restrictions	None.

Example usage

To display all of the commands in the CLI:

```
DES-3250:4#?
..
?
clear
clear arptable
clear counters
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
```

```
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config admin local_enable
config arp_aging time
config arpentry
config authen application
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

dir	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	**dir**
Description	This command will display all of the commands available through the Command Line Interface (CLI).
Parameters	None.
Restrictions	None.

Example usage:

To display all commands:

```
DES-3250:4#dir
..
?
clear
clear arptable
clear counters
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
```

```
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config admin local_enable
config arp_aging time
config arpentry
config authen application
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config command_history

Purpose	Used to configure the command history.
Syntax	**config command_history <value 1-40>**
Description	This command is used to configure the command history.
Parameters	*<value 1-40>* – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	None.

Example usage

To configure the command history:

```
DES-3250:4#config command_history 20
Command: config command_history 20

Success.

DES-3250:4#
```

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-3250:4#show command_history
Command: show command_history

?
? show
show vlan
show command history

DES-3250:4#
```

clear

Purpose	Used to clear CLI screen.
Syntax	**clear**
Description	This command will clear the command CLI screen.
Parameters	None.
Restrictions	None.

Example usage

To clear the command history:

```
DES-3250:4#clear
```

A

TECHNICAL SPECIFICATIONS

Physical and Environmental	
AC Input & External Redundant Power Supply:	100 - 240 VAC, 50-60 Hz (internal universal power supply) Redundant power supply – will take over when internal power supply fails.
Power Consumption:	90 watts maximum
DC Fans:	2 built-in 40 x 40 x10 mm fans
Operating Temperature:	0 to 40 degrees Celsius (32 to 104 degrees Fahrenheit)
Storage Temperature:	-40 to 70 degrees Celsius (-40 to 158 degrees Fahrenheit)
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width
Weight:	3.15 kg
EMC:	CE Class A FCC Class A C-Tick
Safety:	CSA International

General	
Standards:	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1D Spanning Tree IEEE 802.1W Rapid Spanning Tree IEEE 802.1 P/Q VLAN IEEE 802.1p Priority Queues IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation
Protocols:	CSMA/CD
Data Transfer Rates: Ethernet Fast Ethernet Gigabit Ethernet Fiber Optic	Half-duplex Full-duplex 10 Mbps 20Mbps 100Mbps 200Mbps n/a 2000Mbps SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver)
Network Cables: 10BASE-T:	UTP Cat.5, Cat.5 Enhanced for 1000Mbps UTP Cat.5 for 100Mbps

100BASE-TX:	UTP Cat.3, 4, 5 for 10Mbps EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)
Number of Ports:	48 x 10/100 Mbps NWay ports 2 Gigabit Ethernet

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	16 MB per device
Filtering Address Table:	8K MAC address per device
Packet Filtering / Forwarding Rate:	Full-wire speed for all connections. 148,810 pps per port (for 100Mbps) 1,488,100 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 10 - 1000000 seconds. Default = 300.