D-Link
Building Networks for People

XSTACK

CLI Manual

Product Model : xStack™ DES-3526/DES-3526DC/DES-3550

Layer 2 Managed Stackable Fast Ethernet Switch

Release 4

Table of Contents

INTRODUCTION 1

USING THE CONSOLE CLI 4

COMMAND SYNTAX 8

BASIC SWITCH COMMANDS 10

MODIFY BANNER AND PROMPT COMMANDS 20

SWITCH PORT COMMANDS 24

PORT SECURITY COMMANDS 27

NETWORK MANAGEMENT (SNMP) COMMANDS 31

SWITCH UTILITY COMMANDS 50

NETWORK MONITORING COMMANDS 58

MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS 70

FORWARDING DATABASE COMMANDS 82

TRAFFIC CONTROL COMMANDS 89

QOS COMMANDS 94

PORT MIRRORING COMMANDS 101

VLAN COMMANDS 104

ASYMMETRIC VLAN COMMANDS 109

LINK AGGREGATION COMMANDS 111

IP-MAC BINDING 116

LIMITED IP MULTICAST ADDRESS 124

BASIC IP COMMANDS 126

IGMP SNOOPING COMMANDS 129

DHCP RELAY 137

802.1X COMMANDS 142

ACCESS CONTROL LIST (ACL) COMMANDS 153

SAFEGUARD ENGINE COMMANDS 168

TRAFFIC SEGMENTATION COMMANDS 170

TIME AND SNTP COMMANDS 172

ARP COMMANDS 178

ROUTING TABLE COMMANDS 182

MAC NOTIFICATION COMMANDS 184

ACCESS AUTHENTICATION CONTROL COMMANDS 187

SSH COMMANDS 207

SSL COMMANDS 214

D-LINK SINGLE IP MANAGEMENT COMMANDS 220

COMMAND HISTORY LIST 231

TECHNICAL SPECIFICATIONS 234

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.

The DES-3500 Layer 2 stackable Gigabit Ethernet switches are members of the D-Link xStack family. Ranging from 10/100Mbps edge switches to core gigabit switches, the xStack switch family has been future-proof designed to provide a stacking architecture with fault tolerance, flexibility, port density, robust security and maximum throughput with a user-friendly management interface for the networking professional.

This manual provides a reference for all of the commands contained in the CLI for members of the xStack DES-3500 series, including the DES-3526, DES-3526DC, and the DES-3550. Examples present in this manual may refer to any member of the xStack DES-3500 series and may show different port counts, but are universal to this series of switches, unless otherwise stated. Configuration and management of the Switch via the Web-based management agent is discussed in the User's Guide.

Please take note that if this device was purchased outside of Europe, certain cosmetic differences between the actual switch and images in this document will be apparent to the reader, such as the faceplate and the manual cover. The DES-3526/DES-3526DC/DES-3500 has already joined the xStack family for the European market and is soon to be xStack converted, universally. Changes are made to the appearance of the device only and no configuration or internal hardware alterations occur.

Accessing the Switch via the Serial Port

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

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

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

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

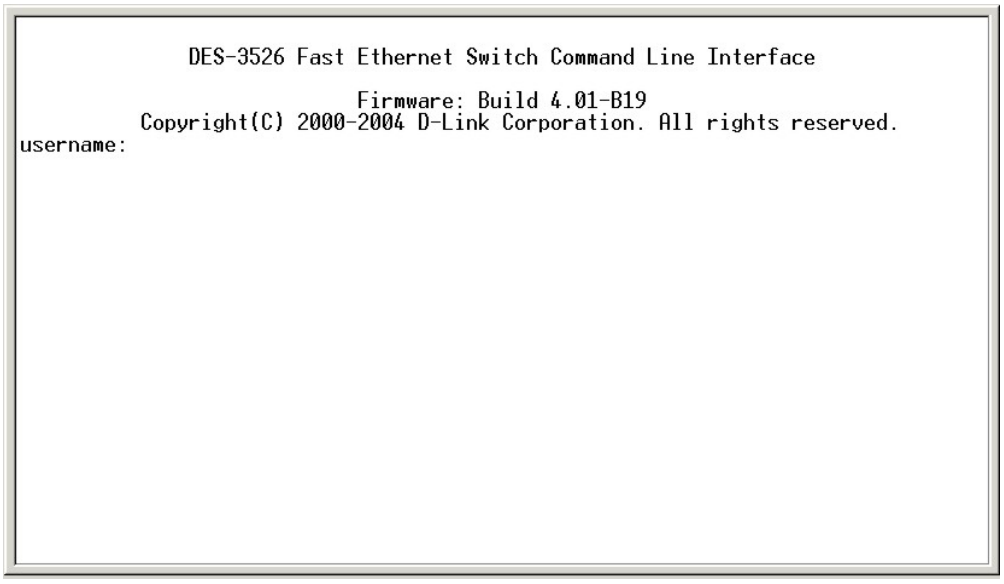

Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-3500:4#**. This is the command line where all commands are input.

Setting the Switch's IP Address

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

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

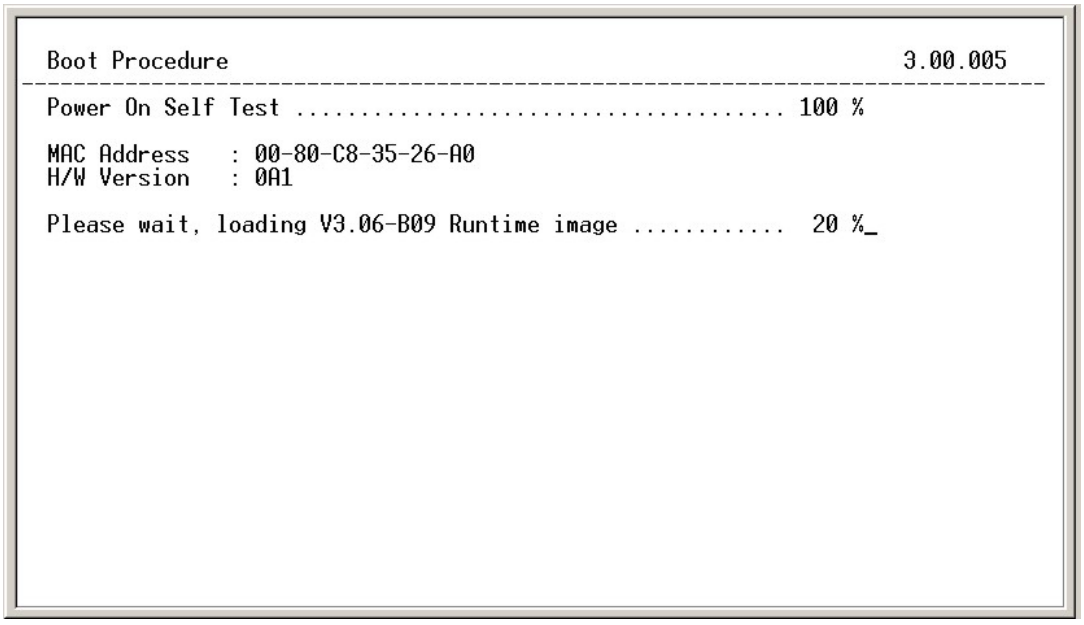

Figure 1-2. Boot Screen

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

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

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

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.
2. Alternatively, users can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

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

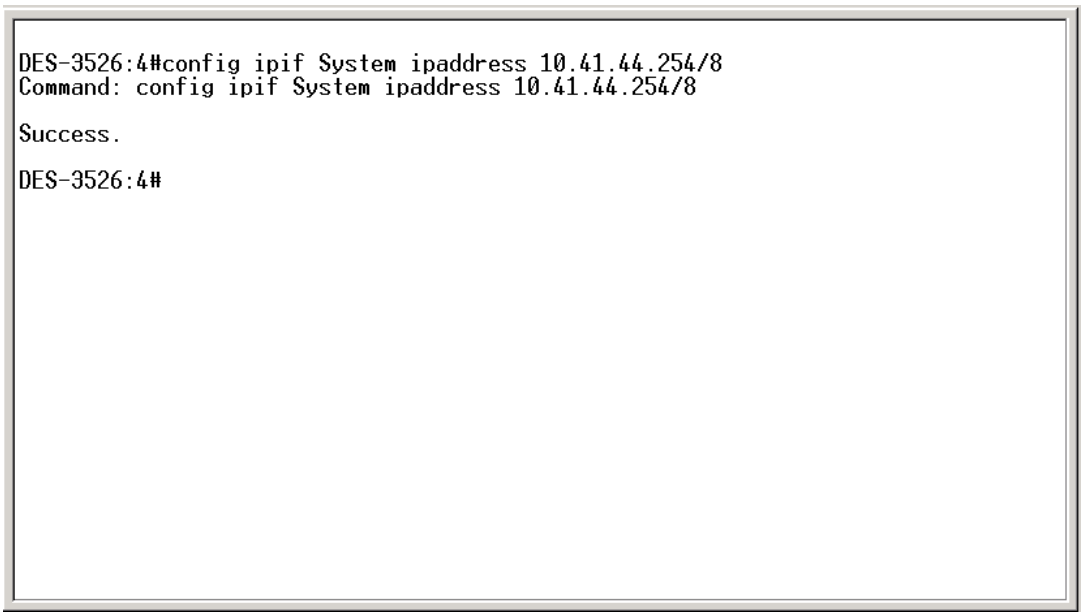

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.41.44.254 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-3500 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**

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

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

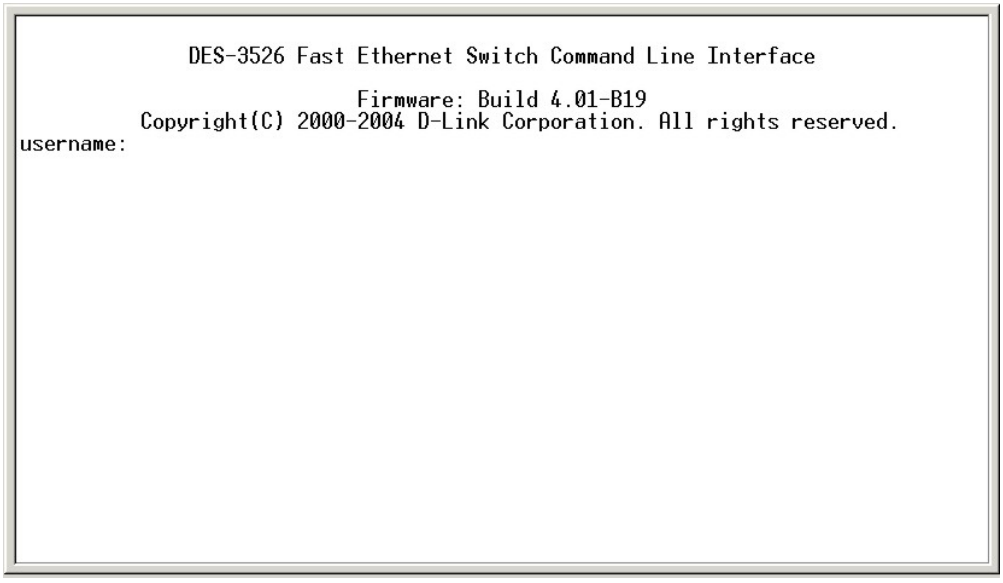

Figure 2-1. Initial Console Screen after logging in

Commands are entered at the command prompt, **DES-3500:4#**.

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

Figure 2-2. The ? Command

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

Figure 2-3. Example Command Parameter Help

In this case, the command **config account** was entered with the parameter **<username>**. The CLI will then prompt users to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

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

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

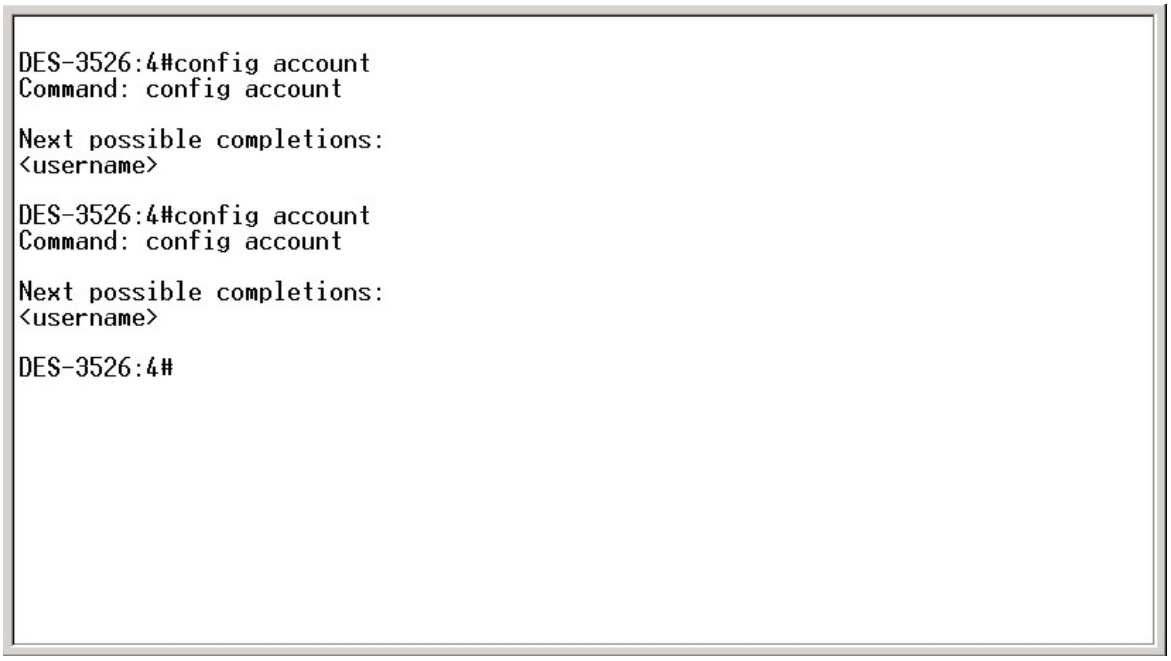

Figure 2-4. Using the Up Arrow to Re-enter a Command

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.

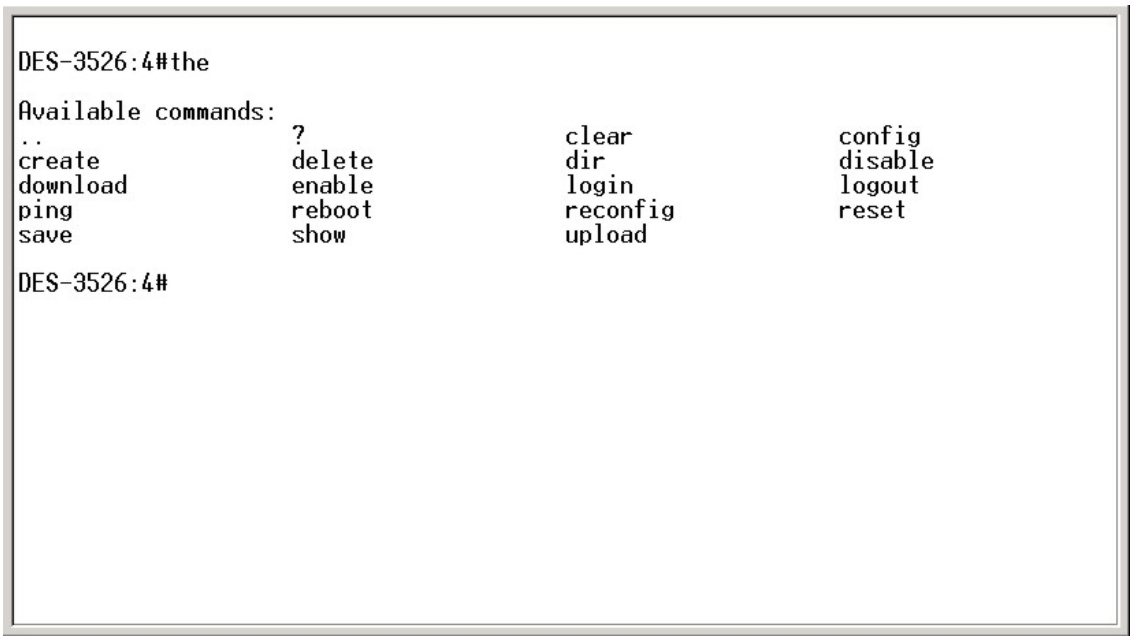

Figure 2-5. The Next Available Commands Prompt

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

```
config arp_aging time

DES-3526:4#show
Command: show

Next possible completions:
802.1p              802.1x              access_profile      account
address_binding     arpentry            asymmetric_vlan     authen
authen_enable       authen_login        authen_policy       autoconfig
bandwidth_control   command_history     config              cpu
cpu_interface_filtering                 dhcp_relay          error
fdb                 firmware            greeting_message    gvrp
igmp_snooping       ipif                iproute             lacp_port
limited             link_aggregation    log                 mac_notification
mirror              multicast           multicast_fdb       packet
port_security       ports               radius              router_ports
safeguard_engine    scheduling          serial_port         session
sim                 snmp                sntp                ssh
ssl                 stp                 switch              syslog
system_severity     time                traffic
traffic_segmentation                    trusted_host        utilization
vlan

DES-3526:4#
```

Figure 2-6. Next possible completions: Show Command

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

3

COMMAND SYNTAX

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

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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable}] | bootp | dhcp]**
Description	In the above syntax example, users must supply an IP interface name in the <ipif_name 12> space, a VLAN name in the <vlan_name 32> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	**config ipif Engineering ipaddress 10.24.22.5/255.0.0.0 vlan Design state enable**

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	**create account [admin | user] <username 15>**
Description	In the above syntax example, users must specify either an **admin** or a **user** level account to be created. Do not type the square brackets.
Example Command	**create account admin Darren**

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

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

{braces}	
	however the effect of the system reset is dependent on which, if any, value is specified. Therefore, with this example there are three possible outcomes of performing a system reset. See the following chapter, Basic Commands for more details about the reset command.
Example command	**reset config**

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

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	
telnet	<ipaddr> {tcp_port <value 0-65535>}
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>*
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-3500:4#create account admin dlink
Command: create account admin dlink

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

Success.

DES-3500:4#
```

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

config account

Purpose	Used to configure user accounts
Syntax	**config account <username>**
Description	The **config account** command configures a user account that has been created using the **create account** command.
Parameters	*<username>*
Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.

Example usage:

To configure the user password of “dlink” account:

```
DES-3500:4#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-3500:4#
```

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-3500:4#show account
Command: show account

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

Total Entries: 1

DES-3500:4#
```

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-3500:4#delete account System
Command: delete account System

Success.

DES-3500:4#
```

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-3500:4#show session
Command: show session

ID  Login Time                 Live Time  From         Level  Name
--  -------------------------  ---------  -----------  -----  -----------
*8  00000 days 00:00:37        03:36:27   Serial Port  4      Anonymous

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

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

Example usage:

To display the Switch's information:

```
DES-3500:4#show switch
Command: show switch

Device Type          : DES-3526 Fast Ethernet Switch
Combo Port           : 1000Base-T + 1000Base-T
MAC Address          : 00-01-02-03-04-00
IP Address           : 10.41.44.22 (Manual)
VLAN Name            : default
Subnet Mask          : 255.0.0.0
Default Gateway      : 0.0.0.0
Boot PROM Version    : Build 3.00.005
Firmware Version     : Build 4.01-B19
Hardware Version     : 0A1
Device S/N           :
Power Status         : Main – Normal, Redundant – Not Present
System Name          : DES-3526
System Location      : 7th_flr_east_cabinet
System Contact       : Julius_Erving_212-555-6666
Spanning Tree        : Disabled
GVRP                 : Disabled
IGMP Snooping        : Disabled
TELNET               : Enabled (TCP 23)
WEB                  : Enabled (TCP 80)
RMON                 : Enabled
Asymmetric VLAN      : Disabled

DES-3500:4#
```

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-3500:4#show serial_port
Command: show serial_port

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

DES-3500:4#
```

config serial_port

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

Example usage:

To configure baud rate:

```
DES-3500:4#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

DES-3500:4#
```

enable clipaging

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

Example usage:

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

```
DES-3500:4#enable clipaging
Command: enable clipaging

Success.

DES-3500:4#
```

disable clipaging

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

Example usage:

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

```
DES-3500:4#disable clipaging
Command: disable clipaging

Success.

DES-3500:4#
```

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-3500:4#enable telnet 23
Command: enable telnet 23

Success.

DES-3500:4#
```

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-3500:4#disable telnet
Command: disable telnet

Success.

DES-3500:4#
```

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

Example usage:

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

```
DES-3500:4#telnet 10.53.13.99 tcp_port 23
Command: telnet 10.53.13.99 tcp_port 23
```

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

Example usage:

To enable HTTP and configure port number:

```
DES-3500:4#enable web 80
Command: enable web 80

Success.

DES-3500:4#
```

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-3500:4#disable web
Command: disable web

Success.

DES-3500:4#
```

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-3500:4#save
Command: save

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

DES-3500:4#
```

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-3500:4#reboot
Command: reboot
Are users 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-3500:4#reset config
Command: reset config
Are users sure to proceed with system reset?(y/n)

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#logout
```

5

MODIFY BANNER AND PROMPT COMMANDS

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

Command	Parameters
config command_ prompt	[<string 16> | username | default]
config greeting_message	{default}
show greeting_message	
enable greeting_message	
disable greeting_message	

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

config command prompt	
Purpose	Used to configure the command prompt.
Syntax	**config command_prompt [<string 16> | username | default]**
Description	Administrator level users can use this command to change the command prompt.
Parameters	*string 16* - The command prompt can be changed by entering a new name of no more that 16 characters. *username* - The command prompt will be changed to the login username. *default* – The command prompt will reset to factory default command prompt.
Restrictions	Only administrator-level users can issue this command. Other restrictions include: • If the "**reset/reset config**" command is executed, the modified command prompt will remain modified. However, the "**reset system**" command will reset the command prompt to the original factory banner.

Example usage

To modify the command prompt to "AtYourService":

```
DGS-3500:4#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:4#
```

config greeting _message	
Purpose	Used to configure the login banner (greeting message).
Syntax	**config greeting _message {default}**
Description	Users can use this command to modify the login banner (greeting message).
Parameters	*default* – If the user enters *default* to the modify banner command, then the banner will be reset to the original factory banner. To open the Banner Editor, click *enter* after typing the **config greeting_message** command. Type the information to be displayed on the banner by using the commands described on the Banner Editor: Quit without save: Ctrl+C Save and quit: Ctrl+W Move cursor: Left/Right/Up/Down Delete line: Ctrl+D Erase all setting: Ctrl+X Reload original setting: Ctrl+L
Restrictions	Only administrator-level users can issue this command. Other restrictions include: • If the "**reset/reset config**" command is executed, the modified banner will remain modified. However, the "**reset system**" command will reset the modified banner to the original factory banner. • The capacity of the banner is 6*80. 6 Lines and 80 characters per line. • Ctrl+W will only save the modified banner in the DRAM. Users need to type the "**save**" command to save it into FLASH. • Only valid in threshold level.

Example usage:

To modify the banner to read "Good evening Mr. Bond.":

```
DGS-3400:4# config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================
                    DGS-3500 Gigabit Ethernet Switch
                        Command Line Interface

                        Firmware: Build 4.01-B19
      Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
================================================================================

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

show greeting_message	
Purpose	Used to view the currently configured greeting message configured on the Switch.
Syntax	**show greeting_message**
Description	This command is used to view the currently configured greeting message on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the currently configured greeting message:

```
DES-3400:4#show greeting_message
Command: show greeting_message

================================================================================
                        DES-3500 Gigabit Ethernet Switch
                            Command Line Interface

                            Firmware: Build 4.01.B19
                  Copyright(C) 2004-2005 D-Link Corporation. All rights reserved.
================================================================================

DES-3400:4#
```

enable greeting_message	
Purpose	Used to enable viewing of the currently configured greeting message configured on the Switch.
Syntax	**enable greeting_message**
Description	This command is used to enable viewing the currently configured greeting message on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To enable viewing of the currently configured greeting message:

```
DES-3400:4#enable greeting_message
Command: enable greeting_message

Success.

DES-3400:4#
```

disable greeting_message	
Purpose	Used to disable viewing of the currently configured greeting message configured on the Switch.
Syntax	**disable greeting_message**
Description	This command is used to disable viewing the currently configured greeting message on the Switch.

disable greeting_message	
Parameters	None.
Restrictions	None.

Example usage:

To disable viewing of the currently configured greeting message:

```
DES-3400:4#disable greeting_message
Command: disable greeting_message

Success.

DES-3400:4#
```

6

SWITCH PORT COMMANDS

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

Command	Parameters
config ports	[<portlist | all>] {speed [auto | 10_half | 10_full |100_half | 100_full | 1000_full]} | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable]} description <desc 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 <desc 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 <desc 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-3500:4#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-3500:4#
```

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-3500:4#show ports
Command show ports

Port   Port       Settings                 Connection               Address
       State      Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    Learning
------ ---------  ---------------------    ---------------------    --------
1      Enabled    Auto/Enabled             Link Down                Enabled
2      Enabled    Auto/Enabled             Link Down                Enabled
3      Enabled    Auto/Enabled             Link Down                Enabled
4      Enabled    Auto/Enabled             Link Down                Enabled
5      Enabled    Auto/Enabled             Link Down                Enabled
6      Enabled    Auto/Enabled             Link Down                Enabled
7      Enabled    Auto/Enabled             Link Down                Enabled
8      Enabled    Auto/Enabled             Link Down                Enabled
9      Enabled    Auto/Enabled             Link Down                Enabled
10     Enabled    Auto/Enabled             100M/Full/None           Enabled
11     Enabled    Auto/Enabled             Link Down                Enabled
12     Enabled    Auto/Enabled             Link Down                Enabled
13     Enabled    Auto/Disabled            Link Down                Enabled
14     Enabled    Auto/Disabled            Link Down                Enabled
15     Enabled    Auto/Disabled            Link Down                Enabled
16     Enabled    Auto/Disabled            Link Down                Enabled
17     Enabled    Auto/Disabled            Link Down                Enabled
18     Enabled    Auto/Disabled            Link Down                Enabled
19     Enabled    Auto/Disabled            Link Down                Enabled
20     Enabled    Auto/Disabled            Link Down                Enabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Example usage:

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

```
DES-3500:4#show ports description
Command: show ports description

Port  Port       Settings                 Connection               Address
      State      Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    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
```

7

PORT SECURITY COMMANDS

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

Command	Parameters
config port_security ports	[<portlist> | all] {admin_state [enable| disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}
delete port_security entry	vlan_name <vlan_name 32> mac_address <macaddr> port <port>
clear port_security_entry	port <portlist>
show port_security	{ports <portlist>}
enable port_security trap_log	
disable port_security trap_log	

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

config port_security ports

Purpose	Used to configure port security settings.
Syntax	**config port_security ports [<portlist> | all] {admin_state [enable| disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}**
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 0-64>* - 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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the port security:

```
DES-3500:4#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-3500:4#
```

delete port_security_entry

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

Example usage:

To delete a port security entry:

```
DES-3500:4#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-3500:4#
```

clear port_security_entry

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

Example usage:

To clear a port security entry by port:

```
DES-3500:4# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DES-3500:4#
```

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-3500:4#show port_security ports 1-5
Command: show port_security ports 1-5

Port_security Trap/Log : Disabled
Port  Admin State   Max. Learning Addr.   Lock Address Mode
----  -----------   -------------------   -----------------
1     Disabled      1                     DeleteOnReset
2     Disabled      1                     DeleteOnReset
3     Disabled      1                     DeleteOnReset
4     Disabled      1                     DeleteOnReset
5     Disabled      1                     DeleteOnReset

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

enable port_security trap_log

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

Example usage:

To enable the port security trap log setting:

```
DES-3500:4#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3500:4#
```

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

Example usage:

To enable the port security trap log setting:

```
DES-3500:4#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3500:4#
```

8

NETWORK MANAGEMENT (SNMP) COMMANDS

The DES-3500 Switch series supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. Users can specify which version of the SNMP users want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

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

Command	Parameters
create snmp user	<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	<username 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included | excluded]
delete snmp view	<view_name 32> [all | oid]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community	<community_string 32>
show snmp community	<community_string 32>
config snmp engineID	<snmp_engineID>
show snmp engineID	
create snmp group	<groupname 32> {v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]} {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	<ipaddr> {v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]} <auth_string 32>

Command	Parameters
delete snmp host	<ipaddr>
show snmp host	<ipaddr>
create trusted_host	<ipaddr>
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.
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:

create snmp user	
	• <*auth password 8-16*> - An alphanumeric sting of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host. • <*auth_key 32-32*> - Enter an alphanumeric sting of exactly 32 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host. • *sha* – Specifies that the HMAC-SHA-96 authentication level will be used. • <*auth password 8-20*> - An alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host. • <*auth_key 40-40*> - Enter an alphanumeric sting of exactly 40 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host. *priv* – Adding the priv (privacy) parameter will allow for encryption in addition to the authentication algorithm for higher security. The user may choose: • des – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using: • <*priv_password 8-16*> - An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent. • <*priv_key 32-32*> - Enter an alphanumeric key string of exactly 32 characters, in hex form, that will be used to encrypt the contents of messages the host sends to the agent. • *none* – Adding this parameter will add no encryption.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DES-3500:4#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-3500:4#
```

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

Example usage:

To delete a previously entered SNMP user on the Switch:

```
DES-3500:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-3500:4#
```

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-3500:4#show snmp user
Command: show snmp user

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

Total Entries: 1

DES-3500:4#
```

create snmp view

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

Example usage:

To create an SNMP view:

```
DES-3500:4#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-3500:4#
```

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-3500:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#
```

create snmp community

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

Example usage:

To create the SNMP community string "dlink:"

```
DES-3500:4#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DES-3500:4#
```

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-3500:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#
```

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-3500:4#config snmp 0035636666
Command: config snmp engineID 0035636666

Success.

DES-3500:4#
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the Switch.
Syntax	**show snmp engineID**
Description	The **show snmp engineID** command displays the identification of the SNMP engine on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the current name of the SNMP engine on the Switch:

```
DES-3500:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DES-3500:4#
```

create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	**create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}**
Description	The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	*<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. *v1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity – Ensures that packets have not been tampered with during transit. • Authentication – Determines if an SNMP message is from a valid source. • Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. *write_view* – Specifies that the SNMP group being created has write privileges. *notify_view* – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. • *<view_name 32>* – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP group named "sg1:"

```
DES-3500:4#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-3500:4#
```

delete snmp group

Purpose	Used to remove an SNMP group from the Switch.
Syntax	**delete snmp group <groupname 32>**
Description	The **delete snmp group** command is used to remove an SNMP group from the Switch.
Parameters	*<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the SNMP group named "sg1".

```
DES-3500:4#delete snmp group sg1
Command: delete snmp group sg1

Success.

DES-3500:4#
```

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-3500:4#show snmp groups
Command: show snmp groups
Vacm Access      Table Settings

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

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

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

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

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

Total Entries: 5

DES-3500:4#
```

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

create snmp host	
	Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity – ensures that packets have not been tampered with during transit. • Authentication – determines if an SNMP message is from a valid source. • Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. • *<auth_sting 32>* – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-3500:4#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-3500:4#
```

delete snmp host	
Purpose	Used to remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**delete snmp host <ipaddr>**
Description	The **delete snmp host** command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipaddr>* – The IP address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an SNMP host entry:

```
DES-3500:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DES-3500:4#
```

show snmp host

Purpose	Used to display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp host {<ipaddr>}**
Description	The **show snmp host** command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps that are generated by the Switch's SNMP agent.
Parameters	*<ipaddr>* – The IP address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DES-3500:4#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-3500:4#
```

create trusted_host

Purpose	Used to create the trusted host.
Syntax	**create trusted_host <ipaddr>**
Description	The **create trusted_host** command creates the trusted host. The Switch allows users to specify up to 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-3500:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DES-3500:4#
```

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-3500:4#show trusted_host
Command: show trusted_host

Management Stations

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

Total Entries: 1

DES-3500:4#
```

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-3500:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DES-3500:4#
```

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-3500:4#enable snmp traps
Command: enable snmp traps

Success.

DES-3500:4#
```

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

Example Usage:

To turn on SNMP authentication trap support:

```
DES-3500:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DES-3500:4#
```

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-3500:4#show snmp traps
Command: show snmp traps

SNMP Traps          : Enabled
Authenticate Traps  : Enabled

DES-3500:4#
```

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

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DES-3500:4#disable snmp traps
Command: disable snmp traps

Success.

DES-3500:4#
```

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-3500:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DES-3500:4#
```

config snmp system_contact	
Purpose	Used to enter the name of a contact person who is responsible for the Switch.
Syntax	**config snmp system_contact{<sw_contact>}**
Description	The **config snmp system_contact** command is used to enter the name and/or other information to identify a contact person who is responsible for the Switch. A maximum of 255 character can be used.
Parameters	*<sw_contact>* - A maximum of 255 characters is allowed. A NULL string is accepted if there is no contact.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3500:4#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DES-3500:4#
```

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-3500:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3500:4#
```

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

Example usage:

To configure the Switch name for "**DES-3526 Switch":**

```
DES-3500:4#config snmp system_name DES-3526 Switch
Command: config snmp system_name DES-3526 Switch

Success.

DES-3500:4#
```

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-3500:4#enable rmon
Command: enable rmon

Success.

DES-3500:4#
```

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-3500:4#disable rmon
Command: disable rmon

Success.

DES-3500:4#
```

9

SWITCH UTILITY COMMANDS

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

Command	Parameters
download	[firmware <ipaddr> <path_filename 64> {image_id <int 1-2>} | configuration <ipaddr> <path_filename 64> {increment}]
config firmware	image_id <int 1-2> [delete | boot_up]
show firmware_information	
show config	[current_config | config_in_nvram]
upload	[configuration | log] <ipaddr> <path_filename 64>
enable autoconfig	
disable autoconfig	
show autoconfig	
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> {image_id <int 1-2>} | configuration <ipaddr> <path_filename 64> {increment}]**
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	*firmware* – Download and install new firmware on the Switch from a TFTP server. *configuration* – Download a switch configuration file from a TFTP server. *<ipaddr>* – The IP address of the TFTP server. *<path_filename>* – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3226S.had. *image_id <int 1-2>* - Specify the working section ID. The Switch can hold two firmware versions for the user to select from, which are specified by section ID. *increment* – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only administrator-level users can issue this command.

Example usage:

To download a configuration file:

```
DES-3500:4#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-3500:4#
DES-3500:4##-------------------------------------------------------------------
DES-3500:4##                  DES-3526 Configuration
DES-3500:4##
DES-3500:4##                  Firmware: Build 4.01-B19
DES-3500:4##        Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.
DES-3500:4##-------------------------------------------------------------------
DES-3500:4#
DES-3500:4#
DES-3500:4## BASIC
DES-3500:4#
DES-3500:4#config serial_port baud_rate 9600 auto_logout 10_minutes
Command: config serial_port baud_rate 9600 auto_logout 10_minutes
```

The download configuration command will initiate the loading of the various settings in the order listed in the configuration file. When the file has been successfully loaded the message "End of configuration file for DES-3526" appears followed by the command prompt.

```
DES-3500:4#disable authen_policy
Command: disable authen_policy

Success.

DES-3500:4#
DES-3500:4##-------------------------------------------------------------------
DES-3500:4##            End of configuration file for DES-3526
DES-3500:4##-------------------------------------------------------------------
DES-3500:4#
```

config firmware

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

Example usage:

To configure firmware section 1 as a boot up section:

```
DES-3500:4# config firmware section_id 1 boot_up
Command: config firmware section_id 1 boot_up

Success.

DES-3500:4#
```

show firmware information

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

Example usage:

To display the current firmware information on the Switch:

```
DES-3500:4#show firmware information
Command: show firmware information

ID   Version    Size(B)    Update Time            From                 User
--   --------   -------    -------------------    ------------------   ---------------
 1   2.00-B19   1360471    00000 days 00:00:00    Serial Port (PROM)   Unknown
*2   4.01-B08    2052372   00000 days 00:00:56    10.53.13.94          Anonymous

'*' means boot up section
(T) means firmware update thru TELNET
(S) means firmware update thru SNMP
(W) means firmware update thru WEB
(SIM) means firmware update through Single IP Management

Free space: 3145728 bytes

DES-3500:4#
```

show config

Purpose	Used to display the current or saved version of the configuration settings of the switch.
Syntax	**show config [current_config | config_in_nvram]**
Description	Use this command to display all the configuration settings that are saved to NV RAM or display the configuration settings as they are currently configured. Use the keyboard to list settings one line at a time (Enter), one page at a time (Space) or view all (a). The configuration settings are listed by category in the following order:

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

Example usage:

To view the current configuration settings:

```
DES-3500:4#show config current_config
Command: show config current_config

#-----------------------------------------------------------------
#                   DES-3526 Configuration
#
#                   Firmware: Build 4.01-B19
#       Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.
#-----------------------------------------------------------------


# BASIC

config serial_port baud_rate 9600 auto_logout 10_minutes
enable telnet 23
enable web 80

# STORM

config traffic control 1-5 broadcast disable multicast disable dlf
disable thres
hold 128

# GM

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

upload	
Purpose	Used to upload the current switch settings or the switch history log to a TFTP.
Syntax	**upload [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-3500:4#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-3500:4#
```

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

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

Example usage:

To enable autoconfiguration on the Switch:

```
DES-3500:4#enable autoconfig
Command: enable autoconfig

Success.

DES-3500:4#
```

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

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

```
          DES-3526 Fast Ethernet Switch Command Line Interface

                    Firmware: Build 4.01-B19
        Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.

DES-3500:4#
DES-3500:4#
DES-3500:4#download configuration 10.41.44.44 c:\cfg\setting.txt
Command: download configuration 10.41.44.44 c:\cfg\setting.txt

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

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

```
DES-3500:4#disable authen_policy
Command: disable authen_policy

Success.

DES-3500:4#
DES-3500:4##-------------------------------------------------------------------
DES-3500:4##          End of configuration file for DES-3526
DES-3500:4#

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

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

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

Example usage:

To stop the autoconfiguration function:

```
DES-3500:4#disable autoconfig
Command: disable autoconfig

Success.

DES-3500:4#
```

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

Example usage:

To upload a:

```
DES-3500:4#show autoconfig
Command: show autoconfig
Autoconfig disabled.

Success.

DES-3500:4#
```

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

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DES-3500:4#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-3500:4#
```

10

NETWORK MONITORING COMMANDS

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

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

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

show packet ports

Purpose	Used to display statistics about the packets sent and received by the Switch.
Syntax	**show packet ports <portlist>**
Description	This command is used to display statistics about packets sent and received by ports specified in the *<portlist>*.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

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

```
DES-3500:4#show packet port 2
Command: 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-3500:4#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 | ports {<portlist>}]**
Description	This command will display the real-time port and CPU utilization statistics for the Switch.
Parameters	*cpu* – Entering this parameter will display the current cpu utilization of the Switch. *ports* - Entering this parameter will display the current port utilization of the Switch. ▪ <*portlist*> - Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the port utilization statistics:

```
DES-3500:4#show utilization ports
Command: show utilization ports

Port   TX/sec     RX/sec     Util     Port   TX/sec     RX/sec     Util
------ ---------- ---------- ----     ------ ---------- ---------- ----
1      0          0          0        22     0          0          0
2      0          0          0        23     0          0          0
3      0          0          0        24     0          0          0
4      0          0          0        25     0          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-3500:4#show utilization cpu
Command: show utilization cpu

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

DES-3500:4#
```

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-3500:4#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

DES-3500:4#
```

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

Example usage:

To clear the log information:

```
DES-3500:4#clear log
Command: clear log

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#
```

NOTE: For detailed information regarding Log entries that will appear in this window, please refer to Appendix C at the back of the ***xStack DES-3500 Series Layer 2 Stackable Fast Ethernet Managed Switch User Manual.***

enable syslog

Purpose	Used to enable the system log to be sent to a remote host.
Syntax	**enable syslog**
Description	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-3500:4#enable syslog
Command: enable syslog

Success.

DES-3500:4#
```

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-3500:4#disable syslog
Command: disable syslog

Success.

DES-3500:4#
```

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-3500:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-3500:4#
```

create syslog host	
Purpose	Used to create a new syslog host.
Syntax	**create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]**
Description	The **create syslog host** command is used to create a new syslog host.
Parameters	*<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. *severity* – Severity level indicator. These are described in the following: Bold font indicates that the corresponding severity level is currently supported on the Switch.

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

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

Example usage:

To create syslog host:

```
DES-3500:4#create syslog host 1 severity all facility local0
Command: create syslog host 1 severity all facility local0

Success.

DES-3500:4#
```

config syslog host

Purpose	Used to configure the syslog protocol to send system log data to a remote host.
Syntax	**config syslog host [all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]**
Description	The **config syslog host** command is used to configure the syslog protocol to send system log information to a remote host.
Parameters	*<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. *severity* – Severity level indicator. These are described in the following: **Bold** font indicates that the corresponding severity level is currently supported on the Switch.

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

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.

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

Example usage:

To configure a syslog host:

```
DES-3500:4#config syslog host 1 severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DES-3500:4#
```

Example usage:

To configure a syslog host for all hosts:

```
DES-3500:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DES-3500:4#
```

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-3500:4#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#
```

config system_severity

Purpose	To configure severity level of an alert required for log entry or trap message.
Syntax	**config system_severity [trap | log | all] [critical | warning | information]**
Description	This command is used to configure the system severity levels on the Switch. When an event occurs on the Switch, a message will be sent to the SNMP agent (trap), the Switch's log or both. Events occurring on the Switch are separated into three main categories, these categories are NOT precisely the same as the parameters of the same name (see below). • Information – Events classified as information are basic events occurring on the Switch that are not deemed as problematic, such as enabling or disabling various functions on the Switch. • Warning - Events classified as warning are problematic events that are not critical to the overall function of the Switch but do require attention, such as unsuccessful downloads or uploads and failed logins. • Critical – Events classified as critical are fatal exceptions occurring on the Switch, such as hardware failures or spoofing attacks.
Parameters	Choose one of the following to identify where severity messages are to be sent. • *trap* – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent for analysis. • *log* – Entering this parameter will define which events occurring on the Switch will be sent to the Switch's log for analysis. • *all* – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent and the Switch's log for analysis. Choose one of the following to identify what level of severity warnings are to be sent to the destination entered above. • *critical* – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send only critical events to the Switch's log or SNMP agent. • *warning* – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send critical and warning events to the Switch's log or SNMP agent. • *information* – Entering this parameter along with the proper destination, stated above, will instruct the switch to send informational, warning and critical events to the Switch's log or SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the system severity settings for critical traps only:

```
DES-3500:4#config system_severity trap critical
Command: config system_severity trap critical

Success.

DES-3500:4#
```

11

MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS

This Switch supports three versions of the Spanning Tree Protocol; 802.1d STP, 802.1w Rapid STP and 802.1s MSTP. Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing either of the three spanning tree protocols (STP, RSTP or MSTP). This protocol will also tag BDPU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. These instances will be classified by an *instance_id*. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees. Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

a) A configuration name defined by an alphanumeric string of up to 32 characters (defined in **the config stp mst_config_id** command as *name* <*string*>).

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

c) A 4096 element table (defined here as a *vid_range*) which will associate each of the possible 4096 VLANs supported by the Switch for a given instance.

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

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

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

c) VLANs that will be shared must be added to the MSTP Instance ID (*config stp instance_id*).

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

Command	Parameters
enable stp	
disable stp	
config stp version	[mstp | rstp | stp]
config stp	{maxage <value 6-40> | maxhops <value 1-20> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10> | fbpdu [enable | disable] | lbd [enable | disable] | lbd_recover_timer [0 | <value 60-1000000>]}
config stp ports	<portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-10> | migrate [yes | no] | edge [true | false] | p2p [true | false | auto] | state [enable | disable] | lbd [enable | disable] | fbpdu [enable |disable]}
create stp instance_id	<value 1-4>
config stp instance _id	<value 1-4> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id	<value 1-4>
config stp priority	<value 0-61440> instance_id <value 0-4>
config stp mst_config_id	{revision_level <int 0-65535> | name <string>}
config stp mst_ports	<portlist> instance_id <value 0-4> {internalCost [auto | value 1-200000000] | priority <value 0-240>}
show stp	
show stp ports	{<portlist>}

Command	Parameters
show stp instance	{<value 0-4>}
show stp mst_config id	

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

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

Example usage:

To enable STP, globally, on the Switch:

```
DES-3500:4#enable stp
Command: enable stp

Success.

DES-3500:4#
```

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-3500:4#disable stp
Command: disable stp

Success.

DES-3500:4#
```

config stp version	
Purpose	Used to globally set the version of STP on the Switch.
Syntax	**config stp version [mstp | rstp | stp]**
Description	This command allows the user to choose the version of the spanning tree to be implemented on the Switch.
Parameters	*mstp* – Selecting this parameter will set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. *rstp* - Selecting this parameter will set the Rapid Spanning Tree Protocol

config stp version	
	(RSTP) globally on the Switch. *stp* - Selecting this parameter will set the Spanning Tree Protocol (STP) globally on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3500:4#config stp version mstp
Command: config stp version mstp

Success.

DES-3500:4#
```

config stp	
Purpose	Used to setup STP, RSTP and MSTP on the Switch.
Syntax	**config stp {maxage <value 6-40> | maxhops <value 1-20> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10> | fbpdu [enable | disable] | lbd [enable | disable] | lbd_recover_timer [0 | <value 60-1000000>]}**
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire Switch. All commands here will be implemented for the STP version that is currently set on the Switch.
Parameters	*maxage <value 6-40>* – This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20. *maxhops <value 1-20>* - The number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from 1 to 20. The default is 20. *hellotime <value 1-10>* – The user may set the time interval between transmission of configuration messages by the root device, thus stating that the Switch is still functioning. A time between 1 and 10 seconds may be chosen, with a default setting of 2 seconds.  **NOTE:** In MSTP, the spanning tree is configured by port and therefore, the *hellotime* must be set using the *configure stp ports* command for switches utilizing the Multiple Spanning Tree Protocol. *forwarddelay <value 4-30>* – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds. *txholdcount <1-10>* - The maximum number of BPDU Hello packets transmitted per interval. Default value = 3.

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

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DES-3500:4#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

DES-3500:4#
```

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	**config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-10> | migrate [yes | no] edge [true | false] | p2p [true | false | auto] | state [enable | disable] | lbd [enable | disable] | fbpdu [enable | disable]}**
Description	This command is used to create and configure STP for a group of ports.
Parameters	*<portlist>* – Specifies a range of ports to be configured. *externalCost* – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *auto*. • *auto* – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. • *<value 1-200000000>* - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. *hellotime <value 1-10>* – The time interval between transmission of configuration messages by the designated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and 10 seconds. The default is 2 seconds. *migrate [yes | no]* – Setting this parameter as "*yes*" will set the ports to send out BDPU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1d STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1d network connects to an 802.1w or 802.1s enabled network. Migration should be set as *yes* on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment. *edge [true | false] – true* designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status. *p2p [true | false | auto] – true* indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were *true*. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *false*. The default setting for this parameter is *auto*. *state [enable | disable]* – Allows STP to be enabled or disabled for the ports specified in the port list. The default is *enable*. *lbd [enable | disable]* - Used to enable or disable the loop-back detection function on the switch for the ports configured above in the *config stp* command. *fbpdu [enable | disable]* – When enabled, this allows the forwarding of STP BPDU packets from other network devices when STP is disabled in the specified ports. If users want to enable Forwarding BPDU on a per port basis, the following settings must first be in effect: 1. STP must be globally disabled and 2. Forwarding BPDU must be globally enabled. To globally disable STP, use the **disable stp** command, to globally enable fbpdu, use the **config stp** command. The default is *disable.*
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3500:4#config stp ports 1-5 externalCost 19 hellotime 5 migrate yes state enable
Command: config stp ports 1-5 externalCost 19 hellotime 5 migrate yes state enable

Success.

DES-3500:4#
```

create stp instance_id

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

Example usage:

To create a spanning tree instance 2:

```
DES-3500:4#create stp instance_id 2
Command: create stp instance_id 2

Success.

DES-3500:4#
```

config stp instance_id

Purpose	Used to add or delete an STP instance ID.
Syntax	**config stp instance_id <value 1-4> [add_vlan | remove_vlan] <vidlist>**
Description	This command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an *instance_id*. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 5 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time.  **NOTE:** Switches in the same spanning tree region having the same STP *instance_id* must be mapped identically, and have the same configuration *revision_level* number and the same *name*.
Parameters	<*value 1-4*> - Enter a number between 1 and 4 to define the *instance_id*. The Switch supports 5 STP regions with one unchangeable default instance ID set as *0*. *add_vlan* – Along with the *vid_range* <*vidlist*> parameter, this command will add VIDs to the previously configured STP *instance_id.*

config stp instance_id	
	remove_vlan - Along with the *vid_range* <*vidlist*> parameter, this command will remove VIDs to the previously configured STP *instance_id.* <*vidlist*> - Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DES-3500:4#config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.

DES-3500:4#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DES-3500:4#config stp instance_id 2 remove_vlan 10
Command : config stp instance_id 2 remove_vlan 10

Success.

DES-3500:4#
```

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

Example usage:

To delete STP instance ID 2 from the Switch.

```
DES-3500:4#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DES-3500:4#
```

config stp priority	
Purpose	Used to update the STP instance configuration
Syntax	**config stp priority <value 0-61440> instance_id <value 0-4>**
Description	This command is used to update the STP instance configuration settings on the Switch. The MSTP will utilize the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions will instruct the Switch to give precedence to the selected *instance_id* for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	*priority* <*value 0-61440*> - Select a value between 0 and 61440 to specify the priority for a specified instance ID for forwarding packets. The lower the value, the higher the priority. This entry must be divisible by 4094. *instance_id* <*value 0-4*> - Enter the value corresponding to the previously configured instance ID of which the user wishes to set the priority value. An instance id of *0* denotes the default *instance_id* (CIST) internally set on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3500:4#config stp priority 4096 instance_id 2
Command : config stp priority 4096 instance_id 2

Success.

DES-3500:4#
```

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

Example usage:

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

```
DES-3500:4#config stp mst_config_id revision_level 10 name Trinity
Command : config stp mst_config_id revision_level 10 name Trinity

Success.

DES-3500:4#
```

config stp mst_ports

Purpose	Used to update the port configuration for a MSTP instance.
Syntax	**config stp mst_ports <portlist> instance_id <value 0-4> {internalCost [auto | <value 1-20000000>] priority <value 0-240>**
Description	This command will update the port configuration for a STP *instance_id*. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	<*portlist*> - Specifies a port or range of ports to be configured. *instance_id* <*value 0-4*> - Enter a numerical value between 0 and 4 to identify the *instance_id* previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree. *internalCost* – This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *auto*. There are two options: • *auto* – Selecting this parameter for the internalCost will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • *value 1-2000000* – Selecting this parameter with a value in the range of 1-2000000 will set the quickest route when a loop occurs. A lower *internalCost* represents a quicker transmission. *priority* <*value 0-240*> - Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3500:4#config stp mst_config_id ports 1-5 instance_id 2
internalCost auto priority 16
Command : config stp mst_config_id ports 1-5 instance_id 2
internalCost auto priority 16

Success.

DES-3500:4#
```

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-3500:4#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
Loopback Detection      : Enabled
LBD Recover Time        : 60

DES-3500:4#
```

Status 2 : STP enabled for RSTP

```
DES-3500:4#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
Loopback Detection      : Enabled
LBD Recover Time        : 60

DES-3500:4#
```

Status 3 : STP enabled for MSTP

```
DES-3500:4#show stp
Command: show stp

STP Status              : Enabled
STP Version             : MSTP
Max Age                 : 20
Forward Delay           : 15
Max Age                 : 20
TX Hold Count           : 3
Forwarding BPDU         : Enabled
Loopback Detection      : Enabled
LBD Recover Time        : 60

DES-3500:4#
```

show stp ports	
Purpose	Used to display the Switch's current STP ports configuration.
Syntax	**show stp ports <portlist>**
Description	This command displays the STP ports settings for a specified port or group of ports (one port at a time).
Parameters	*<portlist>* – Specifies a port or range of ports to be viewed. Information for a single port is displayed. If no ports are specified the STP information for port 1 will be displayed. Users may use the Space bar, p and n keys to view information for the remaining ports.
Restrictions	None.

Example usage:

To show STP ports information for port 5 (STP enabled on Switch):

```
DES-3500:4#show stp ports
Command: show stp ports

MSTP Port Information
----------------------
Port Index       : 5     ,  Hello Time: 2 /2 ,  Port STP enabled   LBD : No
External PathCost : Auto/200000   ,  Edge Port : No /No ,  P2P : Auto /Yes
Port Forward BPDU disabled

Msti   Designated Bridge     Internal PathCost  Prio   Status        Role
-----  -------------------   -----------------  ----   ----------    ----------
0      8000/0050BA7120D6  200000             128    Forwarding    Root
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

show stp instance_id	
Purpose	Used to display the Switch's STP instance configuration
Syntax	**show stp instance_id <value 0-4>**
Description	This command displays the Switch's current STP Instance Settings and the STP Instance Operational Status.
Parameters	*<value 0-4>* - Enter a value defining the previously configured *instance_id* on the Switch. An entry of *0* will display the STP configuration for the CIST internally set on the Switch.
Restrictions	None

Example usage:

To display the STP instance configuration for instance 0 (the internal CIST) on the Switch:

```
DES-3500:4#show stp instance 0
Command: show stp instance 0

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

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

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

show stp mst_config_id

Purpose	Used to display the MSTP configuration identification.
Syntax	**show stp mst_config_id**
Description	This command displays the Switch's current MSTP configuration identification.
Parameters	None.
Restrictions	None.

Example usage:

To show the MSTP configuration identification currently set on the Switch:

```
DES-3500:4#show stp mst_config_id
Command: show stp mst_config_id

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

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

DES-3500:4#
```

12

FORWARDING DATABASE COMMANDS

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

Command	Parameters
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> | port <port> | all]
show multicast_fdb	{vlan <vlan_name 32> | mac_address <macaddr>}
show fdb	{port <port> | vlan <vlan_name 32> | 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-3500:4#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-3500:4#
```

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-3500:4#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DES-3500:4#
```

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

Example usage:

To add multicast MAC forwarding:

```
DES-3500:4#config multicast_fdb default 01-00-00-00-00-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1-5

Success.

DES-3500:4#
```

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-3500:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3500:4#
```

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-3500:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3500:4#
```

To delete a multicast FDB entry:

```
DES-3500:4#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DES-3500:4#
```

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

Example usage:

To clear all FDB dynamic entries**:**

```
DES-3500:4#clear fdb all
Command: clear fdb all

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#
```

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-3500:4#show fdb
Command: show fdb

Unicast MAC Address Ageing Time = 300

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

config multicast 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-3500:4#config multicast port_filtering_mode 1-4 forward_all_groups
Command: config multicast port_filtering_mode 1-4 forward_all_groups

Success.

DES-3500:4#
```

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-3500:4#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
```

13

TRAFFIC CONTROL COMMANDS

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

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the **Drop** option of the **Action** field in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the *countdown* field. If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only method of recovering this port is to manually recoup it using the **Port Configuration** window in the **Administration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the **Shutdown** option of the **Action** field in the window below.

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

Command	Parameters
config traffic control	[<storm_grouplist> | all] {broadcast [enable | disable] | multicast [enable | disable] | dlf [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | time_interval <sec 5-30> | countdown [0 | <minute 5-30>]}
show traffic control	show traffic control {[group_list <storm_grouplist> | port <portlist>]}
config traffic trap	[none | storm_occurred | storm_cleared | both]

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

config traffic control

Purpose	Used to configure broadcast/multicast/dlf packet storm control. The software mechanism is provided to monitor the traffic rate in addition to the hardware storm control mechanism previously provided.
Syntax	**config traffic control [<storm_grouplist> | all] {broadcast [enable | disable] | multicast [enable | disable] | dlf [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | time_interval <sec 5-30> | countdown [0 | <minute 5-30>]}**
Description	This command is used to configure broadcast/multicast/dlf storm control. By adding the new software traffic control mechanism, the user can now use both a hardware and software mechanism, the latter of which will now provide shutdown, recovery and trap notification functions for the Switch.
Parameters	*<storm_grouplist>* – Used to specify a group list of ports to be configured for traffic control, as defined below: Group 1 – Inclusive for ports 1-8. Group 2 - Inclusive for ports 9-16. Group 3 - Inclusive for ports 17-24. Group 4 - Inclusive for ports 9-16 (DES-3550). Inclusive for Gigabit port 25 (DES-3526). Group 5 - Inclusive for ports 33-40 (DES-3550). Inclusive for Gigabit port 26 (DES-3526). Group 6 - Inclusive for ports 41-48 (DES-3550 only).

config traffic control	
	Group 7 - Inclusive for Gigabit port 49 (DES-3550 only). Group 8 - Inclusive for Gigabit port 50 (DES-3550 only). *all* – Specifies all group lists are to be configured for traffic control on the Switch. *broadcast [enable* | *disable]* – Enables or disables broadcast storm control. *multicast [enable* | *disable]* – Enables or disables multicast storm control. *dlf [enable* | *disable]* – Enables or disables dlf traffic control. *action* – Used to configure the action taken when a storm control has been detected on the Switch. The user has two options: • *drop* - Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. • *shutdown* - Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the user manually resets the port using the **config ports enable** command. Choosing this option obligates the user to configure the *time_interval* field as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring. *threshold <value 0-255000>* – The upper threshold at which the specified traffic control is switched on. The *<value>* is the number of broadcast/multicast/dlf packets, in kilopackets per second (Kpps), received by the Switch that will trigger the storm traffic control measures. The default setting is 128000. *time_interval* - The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. *sec 5-30* - The Interval may be set between 5 and 30 seconds with the default setting of 5 seconds. *countdown* - The countdown timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as **shutdown** in the **action** field of this command and therefore will not operate for Hardware based Traffic Control implementations. • *0* - 0 is the default setting for this field and 0 will denote that the port will never shutdown. • *minutes 5-30* – Select a time from 5 to 30 minutes that the Switch will wait before shutting down. Once this time expires and the port is still experiencing packet storms, the port will be placed in shutdown forever mode and can only be manually recovered using the config ports command mentioned previously in this manual.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3500:4# config traffic control 1-12 broadcast enable action shutdown
threshold 1 countdown 10 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown
threshold 1 countdown 10 time_interval 10

Traffic control port_list (shutdown mode) : 1
Warning!
Shutdown mode is incompatible with drop mode in the same block(ex. Port 1-8)

Success.

DES-3500:4#
```

NOTE: When configuring the traffic control for shutdown mode, the *storm_grouplist* will be defined as a port, not as a group of ports. So when the user enters a command like "**config traffic control 1 broadcast enable action shutdown"**, the traffic control shutdown mode will only be configured for port 1, NOT for group 1 (ports 1-8). Any other configuration entered will apply to the *group_list*, not per individual port. The previous example is defining a port list to be configured. The following example defines a group list to be configured.

To configure traffic control and enable broadcast storm control for group_list 1 (ports 1-8):

```
DES-3500:4# config traffic control 1 broadcast enable threshold 10
Command: config traffic control 1 broadcast enable threshold 10

Traffic control port_list (shutdown mode) : 1-8
Warning!
Shutdown mode is incompatible with drop mode in the same block(ex. Port 1-8)

Success.

DES-3500:4#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	**show traffic control {[group_list <storm_grouplist> | port <portlist>]}**
Description	This command displays the current storm traffic control configuration on the Switch.
Parameters	*group_list* <*storm_grouplist*> - Entering this parameter will display the traffic control settings by group list as defined below. Group 1 – Inclusive for ports 1-8. Group 2 - Inclusive for ports 9-16. Group 3 - Inclusive for ports 17-24. Group 4 - Inclusive for ports 9-16 (DES-3550). Inclusive for Gigabit port 25 (DES-3526). Group 5 - Inclusive for ports 33-40 (DES-3550). Inclusive for Gigabit port 26 (DES-3526). Group 6 - Inclusive for ports 41-48 (DES-3550 only). Group 7 - Inclusive for Gigabit port 49 (DES-3550 only). Group 8 - Inclusive for Gigabit port 50 (DES-3550 only). *port* <*portlist*> - Used to specify port or list of ports for which to display traffic control settings. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display traffic control settings for ports 1-3:

```
DES-3500:4#show traffic control port 1-3
Command: show traffic control port 1-3

Traffic Storm Control Trap: None

Port    Broadcast /          Multicast /          DLF /                Time      Count
        Threshold/Action     Threshold            Threshold            Interval  down
        (Action Indication   D: Drop  S: Shutdown *:shudown forever)
------  ---------            ---------            ---------            ----------  ----------
1       Disabled/128000/D    Disabled/128000/D    Disabled/128000/D    5         0
2       Disabled/128000/D    Disabled/128000/D    Disabled/128000/D    5         0
3       Disabled/128000/D    Disabled/128000/D    Disabled/128000/D    5         0

DES-3500:4#
```

To display traffic control settings for group_list 1-3:

```
DES-3500:4#show traffic control group_list 1-3
Command: show traffic control group_list 1-3

Traffic Control

Unit  Group [ports]  Broadcast Storm  Threshold (pps)  Multicast Storm  Threshold (pps)  Destination Lookup Fail  Threshold (pps)
----- ------------------ -------------- ---------------- --------- --------------- ---------------- ----------------
1     1 [1-8]          Disabled       128000           Disabled         128000          Disabled         128000
2     1 [9-16]         Disabled       128000           Disabled         128000          Disabled         128000
3     1 [17-24]        Disabled       128000           Disabled         128000          Disabled         128000

DES-3500:4#
```

config traffic control_trap

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

Example usage:

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

```
DES-3500:4# config traffic control trap both
Command: config traffic control trap both

Success.

DES-3500:4#
```

14

QOS COMMANDS

The DES-3500 switch supports 802.1p priority queuing. The Switch has 4 priority queues. These priority queues are numbered from 3 (Class 3) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

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

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

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

Command	Parameters
config bandwidth_control	[<portlist>] {rx_rate [no_limit | <value 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.
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 Mbits, that the

config bandwidth_control	
	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 Mbits, 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-3500:4#config bandwidth_control 1-10 tx_rate 10
Command: config bandwidth_control 1-10 tx_rate 10

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#
```

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 highest priority queue (hardware queue 3) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received. The *max_packets* parameter allows the user to specify the maximum 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 highest 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 users 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-3500:4# config scheduling 0 max_packet 100 max_latency 150
Command: config scheduling 0 max_packet 100 max_latency 150

Success.

DES-3500:4#
```

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-3500:4# 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-3500:4#
```

config 802.1p user_priority

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

802.1p	Hardware Queue	Remark
0	1	Mid-low
1	0	Lowest
2	0	Lowest
3	1	Mid-low
4	2	Mid-high
5	2	Mid-high
6	3	Highest
7	3	Highest.

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

Example usage:

To configure 802.1 user priority on the Switch:

```
DES-3500:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-3500:4#
```

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

Example usage:

To show 802.1p user priority:

```
DES-3500:4# 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-3500:4#
```

config 802.1p default_priority	
Purpose	Used to configure the 802.1p default priority settings on the Switch. If an untagged packet is received by the Switch, the priority configured with this command will be written to the packet's priority field.
Syntax	**config 802.1p default_priority [<portlist> | all] <priority 0-7>**
Description	This command allows the user to specify default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine 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 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-3500:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3500:4#
```

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-3500:4# 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-3500:4#
```

15

PORT MIRRORING COMMANDS

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

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

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

config mirror port	
Purpose	Used to configure a mirror port – source port pair on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe can then be attached to study the traffic crossing the source port in a completely obtrusive manner.
Syntax	**config mirror port <port> [add | delete] source ports <portlist> [rx | tx | both]**
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, users can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	*<port>* – This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be operating at the same speed 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. *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-3500:4# config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

DES-3500:4#
```

Example usage:

To delete the mirroring ports:

```
DES-3500:4#config mirror port 1 delete source port 2-4
Command: config mirror 1 delete source 2-4

Success.

DES-3500:4#
```

enable mirror

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

Example usage:

To enable mirroring configurations:

```
DES-3500:4#enable mirror
Command: enable mirror

Success.

DES-3500:4#
```

disable mirror

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

Example usage:

To disable mirroring configurations:

```
DES-3500:4#disable mirror
Command: disable mirror

Success.

DES-3500:4#
```

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-3500:4#show mirror
Command: show mirror

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

DES-3500:4#
```

16

VLAN COMMANDS

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

Command	Parameters
create vlan	<vlan_name 32> {tag <vlanid 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 the user 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. Up to 255 static VLANs may be created per configuration. Only administrator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DES-3500:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DES-3500:4#
```

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

Example usage:

To remove the VLAN "v1":

```
DES-3500:4#delete vlan v1
Command: delete vlan v1

Success.

DES-3500:4#
```

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

Example usage:

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

```
DES-3500:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DES-3500:4#
```

To delete ports from a VLAN:

```
DES-3500:4#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.

DES-3500:4#
```

config gvrp

Purpose	Used to configure GVRP on the Switch.
Syntax	**config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}**
Description	This command is used to configure the Group VLAN Registration Protocol on the Switch. Ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID) can be configured.
Parameters	*<portlist>* – A port or range of ports for which users want to enable GVRP for. *all* – Specifies all of the ports on the Switch. *state [enable | disable]* – Enables or disables GVRP for the ports specified in the port list. *ingress_checking [enable | disable]* – Enables or disables ingress checking for the specified port list. *acceptable_frame [tagged_only | admit_all]* – This parameter states the frame type that will be accepted by the Switch for this function. *tagged_only* implies that only VLAN tagged frames will be accepted, while *admit_all* implies tagged and untagged frames will be accepted by the Switch. *pvid <vlanid 1-4094>* – Specifies the default VLAN associated with the port.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3500:4#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-3500:4#
```

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-3500:4#enable gvrp
Command: enable gvrp

Success.

DES-3500:4#
```

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-3500:4#disable gvrp
Command: disable gvrp

Success.

DES-3500:4#
```

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 to display a summary of settings.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DES-3500:4#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-3500:4#
```

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-3500:4#show gvrp 1-10
Command: show gvrp 1-10

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

Total Entries : 10

DES-3500:4#
```

17

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-3500:4#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DES-3500:4#
```

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-3500:4#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DES-3500:4#
```

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 currently set on the Switch:

```
DES-3500:4#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN: Enabled

DES-3500:4#
```

18

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <value 1-6> {type [lacp | static]}
delete link_aggregation	group_id <value 1-6>
config link_aggregation	group_id <value 1-6> {master_port <port> | ports <portlist> state [enable | disable]}
config link_aggregation algorithm	[mac_source | mac_destination | mac_source_dest | 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	*<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-3500:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DES-3500:4#
```

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

Example usage:

To delete link aggregation group:

```
DES-3500:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DES-3500:4#
```

config link_aggregation	
Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-6> {master_port <port> | ports <portlist> | state [enable | disable]**
Description	This command allows users to configure a link aggregation group that was created with the **create link_aggregation** command above. The DES-3500 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. *master_port <port>* – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. *ports <portlist>* – Specifies a port or range of ports that will belong to the link aggregation group. *state [enable | disable]* – Allows users to enable or disable the specified link aggregation group.
Restrictions	Only administrator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

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

```
DES-3500:4#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-3500:4#
```

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 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-3500:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3500:4#
```

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

Example usage:

To display Link Aggregation configuration:

```
DES-3500:4#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-3500:4#
```

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-3500:4#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DES-3500:4#
```

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

Example usage:

To display LACP port mode settings:

```
DES-3500:4#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-3500:4#
```

19

IP-MAC BINDING

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the DES-3500 series, the maximum number of IP-MAC Binding entries is 512. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

ACL Mode

Due to some special cases that have arisen with the IP-MAC binding, this Switch has been equipped with a special ACL Mode for IP-MAC Binding, which should alleviate this problem for users. When enabled, the Switch will create two entries in the Access Profile Table. The entries may only be created if there are at least two Profile IDs available on the Switch. If not, when the ACL Mode is enabled, an error message will be prompted to the user. When the ACL Mode is enabled, the Switch will only accept packets from a created entry in the IP-MAC Binding Setting window. All others will be discarded.

To configure the ACL mode, the user must first create an IP-MAC binding using the **create address_binding ip_mac ipaddress** command and select the mode as *acl*. Then the user must enable the mode by entering the **enable address_binding acl_mode** command. If an IP-MAC binding entry is created and the user wishes to change it to an ACL mode entry, the user may use the **config address_binding ip_mac ipaddress** command and select the mode as *acl*.

NOTE: When configuring the ACL mode function of the IP-MAC binding function, please pay close attention to previously set ACL entries. Since the ACL mode entries will fill the first two available access profiles and access profile IDs denote the ACL priority, the ACL mode entries may take precedence over other configured ACL entries. This may render some user-defined ACL parameters inoperable due to the overlapping of settings combined with the ACL entry priority (defined by profile ID). For more information on ACL settings, please see "Configuring the Access Profile" section mentioned previously in this chapter.

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

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

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

Command	Parameters
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode {arp | acl]}
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode {arp | acl]}
config address_binding ip_mac ports	[<portlist> | all] state [enable | disable]
show address_binding	[ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]
delete address_binding	[ip-mac [ipaddress <ipaddr> mac_address <macaddr> |all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]
enable address_binding acl_mode	
disable address_binding acl_mode	
enable address_binding trap_log	
disable address_binding trap_log	

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

create address_binding ip_mac ipaddress

Purpose	Used to create an IP-MAC Binding entry.
Syntax	**<ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode {arp | acl]}**
Description	This command will create an IP-MAC Binding entry.
Parameters	<*ipaddr*> The IP address of the device where the IP-MAC binding is made. <*macaddr*> The MAC address of the device where the IP-MAC binding is made. <*portlist*> - Specifies a port or range of ports to be configured for address binding. *all* – Specifies that all ports on the switch will be configured for address binding. *mode* – The user may set the mode for this IP-MAC binding settings by choosing one of the following: • *arp* - Choosing this selection will set a normal IP-MAC Binding entry for the IP address and MAC address entered. • *acl* - Choosing this entry will allow only packets from the source IP-MAC binding entry created here. All other packets with a different IP address will be discarded by the Switch. This mode can only be used if the ACL Mode has been enabled in the IP-MAC Binding Ports window as seen previously.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DES-3500:4#create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04
Command: create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04

Success.

DES-3500:4#
```

To create address binding on the Switch for ACL mode:

```
DES-3500:4#create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04 mode acl
Command: create address_binding ip_mac ipaddress 10.1.1.3 mac_address
00-00-00-00-00-04 mode acl

Success.

DES-3500:4#
```

Once the ACL mode has been created and enabled (without previously created access profiles), the access profile table will look like this:

```
DES-3500:4#show access_profile
Command: show access_profile

Access Profile Table

Access Profile ID : 1
Type      : Packet Content Filter
Owner     : Address_binding
Masks     :
Offset 0-15    : 0x00000000 0000ffff    ffffffff       00000000
Offset 16-31   : 0x00000000 00000000  00000000  0000ffff
Offset 32-47   : 0xffff0000    00000000  00000000  00000000
Offset 48-63   : 0x00000000 00000000  00000000  00000000
Offset 64-79   : 0x00000000 00000000  00000000  00000000

Access ID  : 1
Mode       : Permit
Owner      : Address_binding
Port       : 1
-------------------------------------------------------------------------------
Offset 0-15    : 0x00000000 0000ffff    ffffffff       00000000
Offset 16-31   : 0x00000000 00000000  00000000  0000ffff
Offset 32-47   : 0xffff0000    00000000  00000000  00000000
Offset 48-63   : 0x00000000 00000000  00000000  00000000
Offset 64-79   : 0x00000000 00000000  00000000  00000000
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

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

config address_binding ip_mac ipaddress	
Purpose	Used to configure an IP-MAC Binding entry.
Syntax	**<ipaddr> mac_address <macaddr> {ports [<portlist> | all] | mode {arp | acl]}**
Description	This command will configure an IP-MAC Binding entry.
Parameters	<*ipaddr*> - The IP address of the device where the IP-MAC binding is made. <*macaddr*> - The MAC address of the device where the IP-MAC binding is made. <*portlist*> - Specifies a port or range of ports to be configured for address binding. *all* – Specifies that all ports on the switch will be configured for address binding. *mode* – The user may set the mode for this IP-MAC binding settings by choosing one of the following: • *arp* - Choosing this selection will set a normal IP-MAC Binding entry for the IP address and MAC address entered. • *acl* - Choosing this entry will allow only packets from the source IP-MAC binding entry created here. All other packets with a different IP address will be discarded by the Switch. This mode can only be used if the ACL Mode has been enabled in the IP-MAC Binding Ports window as seen previously.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3500:4#config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05
Command: config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05

Success.

DES-3500:4#
```

To configure address binding on the Switch for ACL mode:

```
DES-3500:4#config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05 mode acl
Command: config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05 mode acl

Success.

DES-3500:4#
```

config address_binding ip_mac ports	
Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.
Syntax	**[<portlist> | all] state [enable | disable]**
Description	This command will configure IP-MAC state to enable or disable for specified ports.
Parameters	<*portlist*> – Specifies a port or range of ports. *all* – specifies all ports on the switch.

config address_binding ip_mac ports	
	state [enable | *disable]* – Enables or disables the specified range of ports.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3500:4#config address_binding ip_mac ports 2 state enable
Command: config address_binding ip_mac ports 2 state enable

Success.

DES-3500:4#
```

show address_binding	
Purpose	Used to display IP-MAC Binding entries.
Syntax	**[ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]**
Description	This command will display IP-MAC Binding entries. Three different kinds of information can be viewed. • *ip_mac* – Address Binding entries can be viewed by entering the physical and IP addresses of the device. • *blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the physical address of the device. • *ports* - The number of enabled ports on a device.
Parameters	*all* – For IP_MAC binding *all* specifies all the IP-MAC binding entries; for Blocked Address Binding entries *all* specifies all the blocked VLANs and their bound physical addresses. <*ipaddr*> The IP address of the device where the IP-MAC binding is made. <*macaddr*> The MAC address of the device where the IP-MAC binding is made. <*vlan_name*> The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.
Restrictions	None

Example usage:

To show IP-MAC Binding on the switch:

```
DES-3500:4#show address_binding ip_mac ipaddress 10.1.1.8
mac_address 00-00-00-00-00-12
Command: show address_binding ip_mac ipaddress 10.1.1.8
mac_address 00-00-00-00-00-12

ACL_mode : Enabled
Trap/Log    : Disabled
Enabled ports: 2

IP Address      MAC Address           Ports       Status     Mode
--------------  --------------------  ----------  ---------  ---------
10.1.1.8        00-00-00-00-00-12     1-26        Active     ACL

Total entries : 1

DES-3500:4#
```

delete address_binding

Purpose	Used to delete IP-MAC Binding entries.
Syntax	**[ip-mac [ipaddress <ipaddr> mac_address <macaddr> | all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]**
Description	This command will delete IP-MAC Binding entries. Two different kinds of information can be deleted. • *IP_MAC* –Individual Address Binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to *all* will delete all the Address Binding entries. • *Blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the physical address of the device. To delete all the Blocked Address Binding entries, toggle *all.*
Parameters	<*ipaddr*> The IP address of the device where the IP-MAC binding is made. <*macaddr*> The MAC address of the device where the IP-MAC binding is made. <*vlan_name*> The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN. *all* – For IP_MAC binding *all* specifies all the IP-MAC binding entries; for Blocked Address Binding entries *all* specifies all the blocked VLANs and their bound physical addresses.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an IP-MAC Binding on the Switch:

```
DES-3500:4#delete address-binding ip-mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-06
Command: delete address-binding ip-mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-06

Success.

DES-3500:4#
```

enable address_binding acl_mode	
Purpose	Used to enable the ACL mode for an IP-MAC binding entry.
Syntax	**enable address_binding acl_mode**
Description	This command, along with the **disable address_binding acl_mode** will enable and disable the ACL mode for IP-MAC binding on the Switch, without altering previously set configurations. When enabled, the Switch will automatically create two ACL packet content mask entries that can be viewed using the **show access_profile** command. These two ACL entries will aid the user in processing certain IP-MAC binding entries created.
Parameters	None.
Restrictions	Only administrator-level users can issue this command. The ACL entries created when this command is enabled, can only be automatically installed if the Access Profile table has two entries available of the possible 9 entries allowed. These access profile entries can only be deleted using the **disable address_binding acl_mode** and not though the **delete access_profile profile_id** command. Also, the **show config** command will not display the commands for creating the IP-MAC ACL mode access profile entries.

Example usage:

To enable IP-MAC Binding ACL mode on the Switch:

```
DES-3500:4#enable address_binding acl_mode
Command: enable address_binding acl_mode

Success.

DES-3500:4#
```

disable address_binding acl_mode	
Purpose	Used to disable the ACL mode for an IP-MAC binding entry.
Syntax	**disable address_binding acl_mode**
Description	This command, along with the **enable address_binding acl_mode** will enable and disable the ACL mode for IP-MAC binding on the Switch, without altering previously set configurations. When disabled, the Switch will automatically delete two previously created ACL packet content mask entries that can be viewed using the **show access_profile** command.
Parameters	None.
Restrictions	Only administrator-level users can issue this command. The ACL entries created when this command is enabled, can only be automatically installed if the Access Profile table has two entries available of the possible 9 entries allowed. These access profile entries can only be deleted using the **disable address_binding acl_mode** and ***NOT*** though the **delete access_profile profile_id** command. Also, the **show config** command will not display the commands for creating the IP-MAC ACL mode access profile entries.

Example usage:

To disable IP-MAC Binding ACL mode on the Switch:

```
DES-3500:4#disable address_binding acl_mode
Command: disable address_binding acl_mode

Success.

DES-3500:4#
```

enable address_binding trap_log

Purpose	Used to enable the trap log for the IP-MAC binding function.
Syntax	**enable address_binding trap_log**
Description	This command, along with the **disable address_binding trap_log** will enable and disable the sending of trap log messages for IP-MAC binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC binding configuration set on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable sending of IP-MAC Binding trap log messages on the Switch:

```
DES-3500:4#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DES-3500:4#
```

disable address_binding trap_log

Purpose	Used to disable the trap log for the IP-MAC binding function.
Syntax	**disable address_binding trap_log**
Description	This command, along with the **enable address_binding trap_log** will enable and disable the sending of trap log messages for IP-MAC binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC binding configuration set on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable sending of IP-MAC Binding trap log messages on the Switch:

```
DES-3500:4#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DES-3500:4#
```

20

LIMITED IP MULTICAST ADDRESS

The **Limited IP Multicast Range** window allows the user to specify which multicast address(es) reports are to be received on specified ports on the switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the switch. The user may set an IP address or range of IP addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports. The **Limited IP Multicast** Commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config limited multicast address	<portlist> {from <multicast_ipaddr> to <multicast_ipaddr> access [permit | deny] | state [enable | disable]}
delete limited multicast address	[all | <portlist>]
show limited multicast address	{<portlist>}

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

config limited multicast address

Purpose	Used to configure limited IP multicast address range.
Syntax	**config limited multicast address <portlist> {from <multicast_ipaddr> to <multicast_ipaddr> access [permit | deny] | state [enable | disable]}**
Description	The **config limited multicast address** command allows the user to configure the multicast address range, access level, and state.
Parameters	*<portlist>* - A port or range of ports to config the limited multicast address. *from <multicast_ipaddr>* - Enter the lowest multicast IP address of the range. *to <multicast_ipaddr>* - Enter the highest multicast IP address of the range. *access* - Choose either *permit* or *deny* to limit or grant access to a specified range of Multicast addresses on a particular port or range of ports. *state* - This parameter allows the user to *enable* or *disable* the limited multicast address range on a specific port or range of ports.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the limited multicast address on ports 1-3:

```
DES-3500:4#config limited multicast address 1-3 from 224.1.1.1
to 224.1.1.2 access permit state enable
Command: config limited multicast address 1-3 from 224.1.1.1
to 224.1.1.2 access permit state enable

Success.

DES-3500:4#
```

delete limited multicast address

Purpose	Used to delete Limited IP multicast address range.
Syntax	**delete limited multicast address [all | <portlist>]**
Description	The **delete limited multicast address** command allows the user to delete all multicast address ranges or a selected range based on which port or ports the range has been assigned.
Parameters	*all* - Allows the user to delete all limited multicast addresses that have been configured on the Switch. <*portlist*> - Allows the user to delete only those multicast address ranges that have been assigned to a particular port or range of ports.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the limited multicast address on ports 1-3:

```
DES-3500:4#delete limited multicast address 1-3
Command: delete limited multicast address 1-3

Success.

DES-3500:4#
```

show limited multicast address

Purpose	Used to show per-port Limited IP multicast address range.
Syntax	**show limited multicast address {<portlist>}**
Description	The **show limited multicast address command** allows the user to show multicast address range by ports.
Parameters	<*portlist*> - A port or range of ports on which the limited multicast address range to be shown has been assigned.
Restrictions	None.

Example usage:

To show the limited multicast address on ports 1-3:

```
DES-3500:4#show limited multicast address 1-3
Command: show limited multicast address 1-3

Port  From          To            Access    Status
----  ------------  ------------  --------  -------
1     224.1.1.1     224.1.1.2     permit    enable
2     224.1.1.1     224.1.1.2     permit    enable
3     224.1.1.1     224.1.1.2     permit    enable

DES-3500:4#
```

21

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>
enable autoconfig*	

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

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

config ipif

Purpose	Used to configure the System IP interface.
Syntax	**config ipif <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. Users can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *<vlan_name 32>* – The name of the VLAN corresponding to the System IP interface. *state [enable | disable]* – Allows users to enable or disable the IP interface. *bootp* – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface. *dhcp* – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface. If users are using the autoconfig feature, the Switch becomes a DHCP client automatically so it is not necessary to change the ipif settings.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DES-3500:4#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#
```

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

Example usage:

To enable autoconfiguration on the Switch:

```
DES-3500:4#enable autoconfig
Command: enable autoconfig

Success.

DES-3500:4#
```

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

22

IGMP SNOOPING COMMANDS

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

Command	Parameters
config igmp_snooping	[<vlan_name 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>
config router_ports forbidden	<vlan_name 32> [add | delete] <portlist>
enable igmp snooping	forward_mcrouter_only
show igmp snooping	vlan <vlan_name 32>
disable igmp snooping	
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 the user to configure IGMP snooping on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping is to be configured. *host_timeout <sec 1-16711450>* – Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. *router_timeout <sec 1-16711450>* – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. *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 users to enable or disable IGMP snooping for the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-3500:4#config igmp_snooping default host_timeout 250 state enable
Command: config igmp_snooping default host_timeout 250 state enable

Success.

DES-3500:4#
```

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 variable is used in calculating the following IGMP message intervals: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. Users may want to increase this value if a subnet is expected to be lossy. Although 1 is specified as a valid entry, the robustness 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. Users 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-3500:4#config igmp_snooping querier default query_interval 125 state enable
Command: config igmp_snooping querier default query_interval 125 state enable

Success.

DES-3500:4#
```

config router_ports

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

Example usage:

To set up static router ports:

```
DES-3500:4#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DES-3500:4#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden multicast router ports.
Syntax	**config router_ports_forbidden <vlan_name 32> [add | delete] <portlist>**
Description	This command allows designation of a port or range of ports as being forbidden to multicast-enabled routers. This will ensure that multicast packets will not be forwarded to this port – regardless of protocol, etc.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *[add | delete]* - Specifies whether to add or delete forbidden ports of the specified VLAN. *<portlist>* – Specifies a range of ports that will be configured as forbidden router ports.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set up forbidden router ports:

```
DGS-3500:4#config router_ports_forbidden default add 2-10
Command: config router_ports_forbidden default add 2-10

Success.

DGS-3500:4#
```

enable igmp_snooping

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

Example usage:

To enable IGMP snooping on the Switch:

```
DES-3500:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3500:4#
```

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-3500:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3500:4#
```

Example usage:

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

```
DES-3500:4#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only

Success.

DES-3500:4#
```

show igmp_snooping

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

Example usage:

To show IGMP snooping:

```
DES-3500:4#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-3500:4#
```

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

Example usage:

To show IGMP snooping group:

```
DES-3500:4#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-3500:4#
```

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

Example usage:

To display the router ports.

```
DES-3500:4#show router_ports
Command: show router_ports

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

Total Entries: 1

DES-3500:4#
```

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.
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-3500:4#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-3500:4#
```

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-3500:4#show igmp_snooping group
Command: show igmp_snooping group

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

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

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

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

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

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

Total Entries : 6

DES-3500:4#
```

23 DHCP RELAY

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

Command	Parameters
config dhcp_relay	{hops <value 1-16> | time <sec 0-65535>}
config dhcp_relay add ipif	<ipif_name 12> <ipaddr>
config dhcp_relay delete ipif	<ipif_name 12> <ipaddr>
config dhcp_relay option_82 state	[enable | disable]
config dhcp_relay option_82 check	[enable | disable]
config dhcp_relay option_82 policy	[replace | drop | keep]
show dhcp_relay	{ipif <ipif_name 12>}
enable dhcp_relay	
disable dhcp_relay	

Each command is listed in detail in the following sections.

config dhcp_relay

Purpose	Used to configure the DHCP/BOOTP relay feature of the switch.
Syntax	**config dhcp_relay {hops <value 1-16> | time <sec 0-65535>}**
Description	This command is used to configure the DHCP/BOOTP relay feature.
Parameters	*hops <value 1-16>* Specifies the maximum number of relay agent hops that the DHCP packets can cross. *time <sec 0-65535>* If this time is exceeded, the Switch will relay the DHCP packet.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To config DHCP relay:

```
DES-3500:4#config dhcp_relay hops 2 time 23
Command: config dhcp_relay hops 2 time 23

Success.

DES-3500:4#
```

config dhcp_relay add ipif

Purpose	Used to add an IP destination address to the switch's DHCP/BOOTP relay table.
Syntax	**config dhcp_relay add ipif <ipif_name 12> <ipaddr>**
Description	This command adds an IP address as a destination to forward (relay) DHCP/BOOTP relay packets to.
Parameters	*<ipif_name 12>* The name of the IP interface in which DHCP relay is to be enabled. *<ipaddr>* The DHCP server IP address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add an IP destination to the DHCP relay table:

```
DES-3500:4#config dhcp_relay add ipif System 10.58.44.6
Command: config dhcp_relay add ipif System 10.58.44.6

Success.

DES-3500:4#
```

config dhcp_relay delete ipif

Purpose	Used to delete one or all IP destination addresses from the Switch's DHCP/BOOTP relay table.
Syntax	**config dhcp_relay delete ipif <ipif_name 12> <ipaddr>**
Description	This command is used to delete an IP destination addresses in the Switch's DHCP/BOOTP relay table.
Parameters	*<ipif_name 12>* The name of the IP interface that contains the IP address below. *<ipaddr>* The DHCP server IP address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an IP destination from the DHCP relay table:

```
DES-3500:4#config dhcp_relay delete ipif System 10.58.44.6
Command: config dhcp_relay delete ipif System 10.58.44.6

Success.

DES-3500:4#
```

config dhcp_relay option_82 state

Purpose	Used to configure the state of DHCP relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 state [enable | disable]**
Description	This command is used to configure the state of DHCP relay agent information option 82 of the switch.
Parameters	*enable* - When this field is toggled to *Enabled* the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP server and client. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *disable* - If the field is toggled to *disable* the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DES-3500:4#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DES-3500:4#
```

config dhcp_relay option_82 check

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

Example usage:

To configure DHCP relay option 82 check:

```
DES-3500:4#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DES-3500:4#
```

config dhcp_relay option_82 policy

Purpose	Used to configure the reforwarding policy of relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 policy [replace | drop | keep]**
Description	This command is used to configure the reforwarding policy of DHCP relay agent information option 82 of the switch.
Parameters	*replace* - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *drop* - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *keep* - The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 policy:

```
DES-3500:4#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DES-3500:4#
```

show dhcp_relay

Purpose	Used to display the current DHCP/BOOTP relay configuration.
Syntax	**show dhcp_relay {ipif <ipif_name 12>}**
Description	This command will display the current DHCP relay configuration for the Switch, or if an IP interface name is specified, the DHCP relay configuration for that IP interface.
Parameters	*ipif <ipif_name 12>* - The name of the IP interface for which to display the current DHCP relay configuration.
Restrictions	None.

Example usage:

To show the DHCP relay configuration:

```
DES-3500:4#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status                          : Enabled
DHCP/BOOTP Hops Count Limit                      : 2
DHCP/BOOTP Relay Time Threshold                  : 23
DHCP Relay Agent Information Option 82 State     : Enabled
DHCP Relay Agent Information Option 82 Check     : Enabled
DHCP Relay Agent Information Option 82 Policy    : Replace

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

DES-3500:4#
```

Example usage:

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

```
DES-3500:4#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

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

DES-3500:4#
```

enable dhcp_relay

Purpose	Used to enable the DHCP/BOOTP relay function on the Switch.
Syntax	**enable dhcp_relay**
Description	This command is used to enable the DHCP/BOOTP relay function on the Switch.
Parameters	None.

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

Example usage:

To enable DHCP relay:

```
DES-3500:4#enable dhcp_relay
Command: enable dhcp_relay

Success.

DES-3500:4#
```

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

Example usage:

To disable DHCP relay:

```
DES-3500:4#disable dhcp_relay
Command: disable dhcp_relay

Success.

DES-3500:4#
```

24

802.1X COMMANDS

The DES-3500 implements the server-side of the IEEE 802.1x Port-based and MAC-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames.

Command	Parameters
enable 802.1x	
disable 802.1x	
show 802.1x auth_state	{ports <portlist>}
show 802.1x auth_configuration	{ports <portlist>}
config 802.1x capability ports	[<portlist> | all] [authenticator | none]
config 802.1x auth_parameter ports	[<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]
config 802.1x auth_protocol	[radius eap | radius pap]
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 Network Access control server application on the Switch. To select between port-based or MAC-based, use the **config 802.1x auth_mode** command.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable 802.1x switch wide:

```
DES-3500:4#enable 802.1x
Command: enable 802.1x

Success.

DES-3500:4#
```

disable 802.1x

Purpose	Used to disable the 802.1x server on the Switch.
Syntax	**disable 802.1x**
Description	The **disable 802.1x** command is used to disable the 802.1x Network Access control server application on the Switch. To select between port-based or MAC-based, use the **config 802.1x auth_mode** command.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable 802.1x on the Switch:

```
DES-3500:4#disable 802.1x
Command: disable 802.1x

Success.

DES-3500:4#
```

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 user** command is used to display the 802.1x Port-based or MAC-based Network Access control local users currently configured on the Switch.
Parameters	*ports* <*portlist*> – Specifies a port or range of ports to view. The following details are displayed: 802.1x Enabled / Disabled – Shows the current status of 802.1x functions on the Switch. Authentication Mode – Shows the authentication mode, whether it be by MAC address or by port. Authentication Protocol: 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

show 802.1x auth_configuration	
	and transmitting directions, or just the receiving direction. Port Control: ForceAuth / ForceUnauth / Auto – Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized. QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt. TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request / Identity packets. SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request / Identity packets. ServerTimeout – Shows the length of time to wait for a response from a RADIUS server. MaxReq – Shows the maximum number of times to retry sending packets to the supplicant. ReAuthPeriod – Shows the time interval between successive re-authentications. ReAuthenticate: Enabled / Disabled – Shows whether or not to re-authenticate.
Restrictions	None.

Example usage:

To display the 802.1x authentication states:

```
DES-3500:4#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 or MAC-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. Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Restrictions	None.

Example usage:

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

```
DES-3500:4#show 802.1x auth_state
Command: show 802.1x auth_state

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

Example usage:

To display the 802.1x auth state for MAC-based 802.1x:

```
DES-3500:4#show 802.1x auth_state
Command: show 802.1x auth_state

Port number : 1:1
Index   MAC Address         Auth PAE State      Backend State       Port Status
------  ------------------  ------------------  ------------------  ----------------
1       00-08-02-4E-DA-FA   Authenticated       Idle                Authorized
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

config 802.1x auth_mode

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

Example usage:

To configure 802.1x authentication by MAC address:

```
DES-3500:4#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DES-3500:4#
```

config 802.1x capability ports

Purpose	Used to configure the 802.1x capability of a range of ports on the Switch.
Syntax	**config 802.1x capability ports [<portlist> | all] [authenticator | none]**
Description	The **config 802.1x** command has 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.

config 802.1x capability ports	
	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-3500:4#config 802.1x capability ports 1 – 10 authenticator
Command: config 802.1x capability ports 1 – 10 authenticator

Success.

DES-3500:4#
```

config 802.1x auth_parameter	
Purpose	Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	**config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]**
Description	The **config 802.1x auth_parameter** command is used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *all* – Specifies all of the ports on the Switch. *default* – Returns all of the ports in the specified range to their 802.1x default settings. *direction [both | in]* – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction. *port_control* – Configures the administrative control over the authentication process for the range of ports. 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

config 802.1x auth_parameter	
	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-3500:4#config 802.1x auth_parameter ports 1–20 direction both
Command: config 802.1x auth_parameter ports 1–20 direction both

Success.

DES-3500:4#
```

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

Example usage:

To configure the authentication protocol on the Switch:

```
DES-3500:4# config 802.1x auth_protocol radius_pap
Command: config 802.1x auth_protocol radius_pap

Success.

DES-3500:4#
```

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

config 802.1x init	
	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-3500:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-3500:4#
```

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-3500:4#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-3500:4#
```

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 settings:

```
DES-3500:4#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-3500:4#
```

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

Example usage:

To delete previously configured RADIUS server communication settings:

```
DES-3500:4#config radius delete 1
Command: config radius delete 1

Success.

DES-3500:4#
```

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

Example usage:

To configure the RADIUS settings:

```
DES-3500:4#config radius 1 10.48.74.121 key dlink default
Command: config radius 1 10.48.74.121 key dlink default

Success.

DES-3500:4#
```

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-3500:4#show radius
Command: show radius

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

Total Entries : 3

DES-3500:4#
```

25

ACCESS CONTROL LIST (ACL) COMMANDS

The DGS-3500 implements Access Control Lists that enable the Switch to deny network access to specific devices or device groups based on IP settings and MAC address.

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

Note: The ACL command set has been changed for the Release III firmware. In particular, note the different role of the *profile_id* and *access_id* parameters. The new treatment has changed some of the command parameters as well.

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 0x0-0xffff>} | protocol_id_mask <hex 0x0 - 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>}] [profile_id <value 1-255>]
delete access_profile	profile_id <value 1-255>
config access_profile	profile_id <value 1-255> [add access_id <value 1-65535> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {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>}] port <portlist> [permit {priority <value 0-7> {replace_priority} | replace_dscp_with <value 0-63>} | deny] | delete access_id <value 1-65535>]
show access_profile	{profile_id <value 1-255> {access_id <value 1-65535>}}
enable cpu_interface_filtering	
disable cpu_interface_filtering	
create cpu access_profile profile_id	<value 1-5> [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask {<hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>

Command	Parameters
	<hex 0x0-0xffffffff>| offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]
delete cpu access_profile	profile_id <value 1-5>
config cpu access_profile	profile_id <value 1-5> [add access_id <value 1-65535> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} port [<portlist> | all] [permit | deny] | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}]} port [<portlist> | all] [permit | deny] | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} port [<portlist> | all] [permit | deny]] | delete access_id <value 1-65535>]
show cpu access_profile	profile_id <value 1-5>
show cpu_interface_filtering	

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

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

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

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1

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

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

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

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

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

We use the **profile_id 1** which was specified when the access profile was created. The **add** parameter instructs the Switch to add the criteria that follows to the list of rules that are associated with access profile 1. For each rule entered into the access profile,

users can assign an access_id that identifies the rule within the list of rules. The access_id is an index number only and does not effect priority within the profile_id. This access_id may be used later if users want to remove the individual rule from the profile.

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

Due to a chipset limitation, the Switch supports a maximum of 9 access profiles. The rules used to define the access profiles are limited to a total of 800 rules for the Switch.

There is an additional limitation on how the rules are distributed among the Fast Ethernet and Gigabit Ethernet ports. This limitation is described as follows: Fast Ethernet ports are limited to 200 rules for each of the three sequential groups of eight ports. That is, 200 ACL profile rules may be configured for ports 1 to 8. Likewise, 200 rules may be configured for ports 9 to 16, and another 200 rules for ports 17 to 24. Up to 100 rules may be configured for each Gigabit Ethernet port. The table below provides a summary of the maximum ACL profile rule limits.

DES-3526/DES-3526DC

Port Numbers	Maximum ACL Profile Rules per Port Group
1 - 8	200
9 – 16	200
17 - 24	200
25 (Gigabit)	100
26 (Gigabit)	100
Total Rules	800

DES-3550

Port Numbers	Maximum ACL Profile Rules per Port Group
1 - 8	200
9 - 16	200
17 - 24	200
25 - 32	200
33 - 40	200
41 - 48	200
49 (Gigabit)	100
50 (Gigabit)	100
Total Rules	1400

It is important to keep this in mind when setting up VLANs as well. Access rules applied to a VLAN require that a rule be created for each port in the VLAN. For example, let's say VLAN10 contains ports 2, 11 and 12. If users create an access profile specifically for VLAN10, users must create a separate rule for each port. Now take into account the rule limit. The rule limit applies to both port groups 1-8 and 9-16 since VLAN10 spans these groups. One less rule is available for port group 1-8. Two less rules are available for port group 9-16. In addition, a total of three rules apply to the 800 rule Switch limit.

In the example used above - config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny – a single access rule was created. This rule will subtract one rule available for the port group 1 – 8, as well as one rule from the total available rules.

create access_profile

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

create access_profile

0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] [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 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.
- *src_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the source port.
- *dst_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the destination port.
- *flag_mask* – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between *all, urg* (urgent), *ack* (acknowledgement), *psh* (push), *rst* (reset), *syn* (synchronize) and *fin* (finish).

udp – Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field.

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

create access_profile	
	protocol_id <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules • *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header. *packet_content_mask* – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-15* – Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. • *offset_16-31* – Enter a value in hex form to mask the packet from byte 16 to byte 31. • *offset_32*-47 – Enter a value in hex form to mask the packet from byte 32 to byte 47. • offset_48-63 – Enter a value in hex form to mask the packet from byte 48 to byte 63. • offset_64-79 – Enter a value in hex form to mask the packet from byte 64 to byte 79. • *profile_id <value 1-255>* – Sets the relative priority for the profile. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 – 255, yet, remember only 9 access profiles can be created on the Switch
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an access list rules:

```
DES-3500:4#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-3500:4#
```

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. The user may enter a profile ID number between 1 – 255, yet, remember only 9 access profiles can be created on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3500:4# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DES-3500:4#
```

config access_profile

Purpose	Used to configure an access profile on the Switch and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the **create access_profile** command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**config access_profile profile_id <value 1-255> [add access_id <value 1-65535> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {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> <hex 0x0-0xffffffff>}]** **port <portlist> [permit {priority <value 0-7> {replace_priority} | replace_dscp_with <value 0-63>} | deny] | delete access_id <value 1-65535>]**
Description	The **config access_profile** command is used to configure an access profile on the Switch and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the **create access_profile** command, above.
Parameters	*profile_id <value 1-255>* – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 – 255, yet, remember only 9 access profiles can be created on the Switch. • *add access_id <value 1-65535>* – Adds an additional rule to the above specified access profile. The value is used to index the rule created. For information on number of rules that can be created for a given port, lease see the introduction to this chapter. *ethernet* – Specifies that the Switch will look only into the layer 2 part of each packet. • *vlan <vlan_name 32>* – Specifies that the access profile will apply to only to this VLAN. • *source_mac <macaddr>* – Specifies that the access profile will apply to only packets with this source MAC address. • *destination_mac <macaddr>* – Specifies that the access profile will apply to only packets with this destination MAC address. • *802.1p <value 0-7>* – Specifies that the access profile will apply only to packets with this 802.1p priority value. • *ethernet_type <hex 0x0-0xffff>* – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

config access_profile

Parameters

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

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only this VLAN.
- *source_ip <ipaddr>* – Specifies that the access profile will apply to only packets with this source IP address.
- *destination_id <value 0-255>* – Specifies that the access profile will apply to only packets with this destination IP address.
- *dscp <value 0-63>* – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header
- *icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.
  - *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.
  - *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 and if this field contains the value entered here, apply the following rules.

packet_content_mask – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows:

- *offset_0-15* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte.
- *offset_16-31* - Enter a value in hex form to mask the packet from byte 16 to byte 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.

config access_profile

Parameters	*port <portlist>* - Specifies the port number on the Switch to permit or deny access for the rule. *permit* **-** Specifies the rule permit access for incoming packets on the previously specified port. • *priority <value 0-7>* – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header for incoming packets on the previously specified port. • *{replace_priority}* **-** Allows users to specify a new value to be written to the priority field of an incoming packet on the previously specified port. • *replace_dscp_with <value 0-63>* – Allows users to specify a new value to be written to the DSCP field of an incoming packet on the previously specified port. *deny* **-** Specifies the rule will deny access for incoming packets on the previously specified port. *delete access_id <value 1-65535>* - Use this to remove a previously created access rule of a profile ID. For information on number of rules that can be created for a given port, lease see the introduction to this chapter.
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 on port 7 that have IP addresses in the range between 10.42.73.0 to 10.42.73.255:

```
DES-3500:4# config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny

Success.

DES-3500:4#
```

show access_profile

Purpose	Used to display the currently configured access profiles on the Switch.
Syntax	**show access_profile {profile_id <value 1-255> {access_id <value 1-65535>}}**
Description	The **show access_profile** command is used to display the currently configured access profiles.
Parameters	*profile_id* – Specify the profile id to display only the access rules configuration for a single profile ID. The user may enter a profile ID number between 1 – 255, yet, remember only 9 access profiles can be created on the Switch *access_id* - Specify the access ID to display the access rule configuration for the access ID. For information on number of rules that can be created for a given port, please see the introduction to this chapter.
Restrictions	None.

Example usage:

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

```
DES-3500:4#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-3500:4#
```

create cpu access_profile

Purpose	Used to create an access profile specifically for **CPU Interface Filtering** on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.
Syntax	**create cpu access_profile [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xffffffff>} {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] profile_id <value 1-5>**
Description	The **create cpu access_profile** command is used to create an access profile used only for CPU Interface Filtering. Masks can be entered that will be combined with the values the Switch finds in

create cpu access_profile

the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.

Parameters

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

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

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

- *vlan* – Specifies a VLAN mask.
- *source_ip_mask <netmask>* – Specifies an IP address mask for the source IP address.
- *destination_ip_mask <netmask>* – Specifies an IP address mask for the destination IP address.
- *dscp* – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.
- *icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.
  - *type* – Specifies that the Switch will examine each frame's ICMP Type field.
  - *code* – Specifies that the Switch will examine each frame's ICMP Code field.
- *igmp* – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.
  - *type* – Specifies that the Switch will examine each frame's IGMP Type field.
- *tcp* – Specifies that the Switch will examine each frames Transport Control Protocol (TCP) field.
  - *src_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the source port.
  - *dst_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the destination port.
- *flag_mask [all | {urg | ack | psh | rst | syn | fin}]* – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between **all**, **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize) and **fin** (finish).
- *udp* – Specifies that the switch will examine each frame's Universal Datagram Protocol (UDP) field.
  - *src_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the source port.
  - *dst_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the destination port.
- *protocol_id_mask <hex 0x0-0xffffffff>* – Specifies that the Switch will examine each frame's Protocol ID field using the hex form entered here.
  - *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.
- *packet_content_mask* – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows:
  - *offset_0-15* - Enter a value in hex form to mask the packet from byte 0 to byte 15.
  - *offset_16-31* - Enter a value in hex form to mask the packet from byte 16 to byte 31.
  - *offset_32-47* - Enter a value in hex form to mask the packet from byte 32 to byte 47.
  - *offset_48-63* - Enter a value in hex form to mask the packet from byte 48 to byte 63.
  - *offset_64-79* - Enter a value in hex form to mask the packet from byte 64 to byte 79.

profile_id <value 1-5> – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be created with this command.

Restrictions

Only administrator-level users can issue this command.

Example usage:

To create a CPU access profile:

```
DGS-3400:4# create cpu access_profile profile_id 1 ip vlan source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create cpu access_profile profile_id 1 ip vlan source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DGS-3400:4#
```

delete cpu access_profile

Purpose	Used to delete a previously created CPU access profile.
Syntax	**delete cpu access_profile profile_id <value 1-5>**
Description	The **delete cpu access_profile** command is used to delete a previously created CPU access profile.
Parameters	*profile_id* <*value 1-5*> – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3400:4#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DGS-3400:4#
```

config cpu access_profile

Purpose	Used to configure a CPU access profile used for CPU Interface Filtering and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the **create cpu access_profile** command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.
Syntax	**config cpu access_profile profile_id <value 1-5> [add access_id <value 1-65535> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} port [<portlist> | all] | 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 [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>}]} port [<portlist> | all] [permit | deny] | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} port [<portlist> | all] [permit | deny]] | delete access_id <value 1-65535>]**
Description	The **config cpu access_profile** command is used to configure a CPU access profile for

config cpu access_profile

CPU Interface Filtering and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the **create cpu access_profile** command, above.

Parameters

profile_id <value 1-5> – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority.

- *add access_id <value 1-65535>* – Adds an additional rule to the above specified access profile. The value is used to index the rule created.

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

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only to this VLAN.
- *source_mac <macaddr>* – Specifies that the access profile will apply to this source MAC address.
- *destination_mac <macaddr>* – Specifies that the access profile will apply to this destination MAC address.
- *ethernet_type <hex 0x0-0xffff>* – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

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

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only this VLAN.
- *source_ip <ipaddr>* – Specifies that the access profile will apply to only packets with this source IP address.
- *destination_ip <ipaddr>* – Specifies that the access profile will apply to only packets with this destination IP address.
- *dscp <value 0-63>* – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header
- *icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.
    - *type <value 0-255>* – Specifies that the access profile will apply to this ICMP type value.
    - *code <value 0-255>* – Specifies that the access profile will apply to this ICMP code.
- *igmp* – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.
    - *type <value 0-255>* – Specifies that the access profile will apply to packets that have this IGMP type value.
- *tcp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.
    - *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.
    - *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.
- *protocol_id <value 0-255>* – Specifies that the Switch will examine the Protocol field in each packet and if this field contains the value entered here, apply the following rules.
- *udp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.
    - *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this UDP source port in their header.
    - *dst_port <value 0-65535>* – Specifies that the access profile will apply

config cpu access_profile	
Parameters	only to packets that have this UDP destination port in their header. • *protocol_id <value 0-255>* – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules. • *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header. • *packet_content_mask* – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-15* - Enter a value in hex form to mask the packet from byte 0 to byte 15. • *offset_16-31* - Enter a value in hex form to mask the packet from byte 16 to byte 31. • *offset_32-47* - Enter a value in hex form to mask the packet from byte 32 to byte 47. • *offset_48-63* - Enter a value in hex form to mask the packet from byte 48 to byte 63. • *offset_64-79* - Enter a value in hex form to mask the packet from byte 64 to byte 79. *permit* | *deny* – Specify that the packet matching the criteria configured with command will either be permitted or denied entry to the CPU. *delete access_id <value 1-65535>* - Use this to remove a previously created access rule in a profile ID.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure CPU access list entry:

```
DGS-3400:4#config cpu access_profile profile_id 5 add access_id 1
ip vlan default source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3
icmp type 11 code 32 port 1 deny
Command: config cpu access_profile profile_id 10 add access_id 1
ip vlan default source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3
icmp type 11 code 32 port 1 deny

Success.

DGS-3400:4#
```

delete cpu access_profile	
Purpose	Used to delete a previously created CPU access profile.
Syntax	**delete cpu access_profile profile_id <value 1-5>**
Description	The **delete cpu access_profile** command is used to delete a previously created CPU access profile.
Parameters	*profile_id <value 1-5>* – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3400:4#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3400:4#
```

show cpu_access_profile

Purpose	Used to view the CPU access profile entry currently set in the Switch.
Syntax	**show cpu_access_profile {profile_id <value 1-5> {access_id <value 1-65535>}}**
Description	The **show cpu_access_profile** command is used view the current CPU interface filtering entries set on the Switch.
Parameters	*profile_id <value 1-5>* – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command. *access_id <value 1-65535>* - Enter an integer between 1-65535 to define the rule by which to view this profile.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To show the CPU filtering state on the Switch:

```
DGS-3400:4#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Access Profile ID: 1                    TYPE : Ethernet
================================================================================
MASK Option :
VLAN        802.1p
----------  ------
Access ID: 2            Mode: Permit
Ports: 1
--------------------
default
================================================================================
Total Entries: 1

DGS-3400:4#
```

enable cpu_interface_filtering

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

Example Usage:

To enable CPU interface filtering:

```
DES-3500:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3500:4#
```

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

Example Usage:

To disable CPU filtering:

```
DES-3500:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-3500:4#
```

show cpu_interface_filtering	
Purpose	Used to view the current running state of the CPU filtering mechanism on the Switch.
Syntax	**show cpu_interface_filtering**
Description	The **show cpu_interface_filtering** command is used view the current running state of the CPU interface filtering mechanism on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To show the CPU filtering state on the Switch:

```
DES-3500:4#show cpu_interface_filtering
Command: show cpu_interface_filtering

Software ACL Check: Disabled

DES-3500:4#
```

26

SAFEGUARD ENGINE COMMANDS

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the CPU utilization beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter an **Exhausted** mode. When in this mode, the Switch will perform the following tasks to minimize the CPU usage:

a. It will limit bandwidth of receiving ARP packets.
b. It will limit the bandwidth of IP packets received by the Switch.

IP packets may also be limited by the Switch by configuring only certain IP addresses to be accepted. This method can be accomplished through the CPU Interface Filtering mechanism explained in the previous section. Once the user configures these acceptable IP addresses, other packets containing different IP addresses will be dropped by the Switch, thus limiting the bandwidth of IP packets. To keep the process moving fast, be sure not to add many conditions on which to accept these acceptable IP addresses and their packets, this limiting the CPU utilization.

Once in Exhausted mode, the packet flow will decrease by half of the level that caused the Switch to enter Exhausted mode. After the packet flow has stabilized, the rate will initially increase by 25% and then return to a normal packet flow.

NOTICE: When the Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

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

Command	Parameters
config safeguard_engine	{state [enable | disable] | cpu_utilization {rising_threshold <value 20-100> | falling_threshold <value 20-100>} | trap_log [enable | disable]
show safeguard_engine	

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

config safeguard_engine

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

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

Example usage:

To configure the safeguard engine for the Switch:

```
DGS-3500:4#config safeguard_engine state enable cpu_utilization rising_threshold 45
Command: config safeguard_engine state enable cpu_utilization rising_threshold 45

Success.

DGS-3500:4#
```

show safeguard_engine	
Purpose	Used to display current Safeguard Engine settings.
Syntax	**show safeguard_engine**
Description	This will list the current status and type of the Safeguard Engine settings currently configured.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the safeguard engine status:

```
DGS-3500:4#show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State              :  Disabled
Safeguard Engine Current Status  :  Normal mode
=====================================================
CPU utilization information:
Interval                                 : 5 sec
Rising Threshold (20-100)          : 30%
Falling Threshold (20-100)         : 20%
Trap/Log                                 : Disabled

DGS-3500:4#
```

27

TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows users to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied.

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

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

config traffic_segmentation

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

Example usage:

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

```
DES-3500:4# config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DES-3500:4#
```

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-3500:4#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
17      1-26
18      1-26
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

28

TIME AND SNTP COMMANDS

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

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

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

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

Example usage:

To configure SNTP settings:

```
DES-3500:4#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-3500:4#
```

show sntp

Purpose	Used to display the SNTP information.
Syntax	**show sntp**
Description	This command will display SNTP settings information including the source IP address, time and poll interval.
Parameters	None.
Restrictions	None.

Example usage:

To display SNTP configuration information:

```
DES-3500:4#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-3500:4#
```

enable sntp

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

Example usage:

To enable the SNTP function:

```
DES-3500:4#enable sntp
Command: enable sntp

Success.

DES-3500:4#
```

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

Example usage:

To disable SNTP support:

```
DES-3500:4#disable sntp
Command: disable sntp

Success.

DES-3500:4#
```

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

Example usage:

To manually set system time and date settings:

```
DES-3500:4#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3500:4#
```

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-3500:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3500:4#
```

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. *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.

config dst	
Parameters	• <*end_week 1-4,last*> - The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *s_day* – Configure the day of the week in which DST begins. • <*start_day sun-sat*> - The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *e_day* - Configure the day of the week in which DST ends. • <*end_day sun-sat*> - The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *s_mth* - Configure the month in which DST begins. • <*start_mth 1-12*> - The month to begin DST expressed as a number. *e_mth* - Configure the month in which DST ends. • <*end_mth 1-12*> - The month to end DST expressed as a number. *s_time* – Configure the time of day to begin DST. • <*start_time hh:mm*> - Time is expressed using a 24-hour clock, in hours and minutes.
	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-3500:4#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-3500:4#
```

show time	
Purpose	Used to display the current time settings and status.
Syntax	**show time**
Description	This will display system time and date configuration as well as display current system time.
Parameters	None.
Restrictions	None.

Example usage:

To show the time currently set on the Switch's System clock:

```
DES-3500:4#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-3500:4#
```

29

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. The Switch supports up to 255 static ARP entries.

Example Usage:

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

```
DES-3500:4#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-3500:4#
```

config arpentry

Purpose	Used to configure a static entry in the ARP table.
Syntax	**config arpentry <ipaddr> <macaddr>**
Description	This command is used to configure a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the Switch's ARP table.
Parameters	*<ipaddr>* – The IP address of the end node or station. *<macaddr>* – The MAC address corresponding to the IP address above.
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-3500:4#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-3500:4#
```

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-3500:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-3500:4#
```

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-3500:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3500:4#
```

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-3500:4#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-3500:4#
```

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-3500:4#clear arptable
Command: clear arptable

Success.

DES-3500:4#
```

30

ROUTING TABLE COMMANDS

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

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

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

create iproute default

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

Example usage:

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

```
DES-3500:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DES-3500:4#
```

delete iproute default

Purpose	Used to delete a default IP route entry from the Switch's IP routing table.
Syntax	**delete iproute [default]**
Description	This command will delete an existing default entry from the Switch's IP routing table.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the default IP route 10.53.13.254:

```
DES-3500:4#delete iproute default 10.53.13.254
Command: delete iproute default 10.53.13.254

Success.

DES-3500:4#
```

show iproute	
Purpose	Used to display the Switch's current IP routing table.
Syntax	**show iproute**
Description	This command will display the Switch's current IP routing table.
Parameters	None.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DES-3500:4#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-3500:4#
```

31

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-3500:4#enable mac_notification
Command: enable mac_notification

Success.

DES-3500:4#
```

disable mac_notification

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

Example usage:

To disable MAC notification without changing basic configuration:

```
DES-3500:4#disable mac_notification
Command: disable mac_notification

Success.

DES-3500:4#
```

config mac_notification

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

Example usage:

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

```
DES-3500:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DES-3500:4#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist> | all] [enable | disable]**
Description	MAC address notification is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist>* - 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-3500:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-3500:4#
```

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.

show mac_notification	
Parameters	None.
Restrictions	None.

Example usage:

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

```
DES-3500:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State          : Enabled
Interval       : 1
History Size   : 1

DES-3500:4#
```

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-3500:4#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
```

32

ACCESS AUTHENTICATION CONTROL COMMANDS

The TACACS / XTACACS / TACACS+ / RADIUS commands allows secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- TACACS (Terminal Access Controller Access Control System) —Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- Extended TACACS (XTACACS) — An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- TACACS+ (Terminal Access Controller Access Control System plus) — Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery.

The Switch also supports the RADIUS protocol for authentication using the Access Authentication Control commands. RADIUS or Remote Authentication Dial In User Server also uses a remote server for authentication and can be responsible for receiving user connection requests, authenticating the user and returning all configuration information necessary for the client to deliver service through the user. RADIUS may be facilitated on this Switch using the commands listed in this section.

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called a *server host* and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

A) The server verifies the username and password, and the user is granted normal user privileges on the Switch.

B) The server will not accept the username and password and the user is denied access to the Switch.

C) The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in *server groups*, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in *server groups* are used to authenticate users trying to access the Switch. The users will set *server hosts* in a preferable order in the built-in *server group* and when a user tries to gain access to the Switch, the Switch will ask the first *server host* for authentication. If no authentication is made, the second *server host* in the list will be queried, and so on. The built-in *server group* can only have hosts that are running the specified protocol. For example, the TACACS *server group* can only have TACACS *server hosts*.

The administrator for the Switch may set up 5 different authentication techniques per user-defined *method list* (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its *server hosts* and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that user granted access to the Switch will be granted normal user privileges on the Switch. To gain access to admin level privileges, the user must enter the *enable admin* command and then enter a password, which was previously configured by the administrator of the Switch.

NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

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

Command	Parameters
enable authen_policy	
disable authen_policy	
show authen_policy	
create authen_login method_list_name	<string 15>
config authen_login	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name	<string 15>
show authen_login	{default | method_list_name <string 15> | all}
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[default | method_list_name <string 15> | all]
config authen application	{console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application	
create authen server_group	<string 15>
config authen server_group	[tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group	<string 15>
show authen server_group	<string 15>
create authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
delete authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host	
config authen parameter response_timeout	<int 0-255>
config authen parameter attempt	<int 1-255>
show authen parameter	
enable admin	
config admin local_enable	

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

enable authen_policy	
Purpose	Used to enable system access authentication policy.
Syntax	**enable authen_policy**
Description	This command will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the method list and choose a technique for user authentication upon login.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable the system access authentication policy:

```
DES-3500:4#enable authen_policy
Command: enable authen_policy

Success.

DES-3500:4#
```

disable authen_policy	
Purpose	Used to disable system access authentication policy.
Syntax	**disable authen_policy**
Description	This command will disable the administrator-defined authentication policy for users trying to access the Switch. When disabled, the Switch will access the local user account database for username and password verification. In addition, the Switch will now accept the local enable password as the authentication for normal users attempting to access administrator level privileges.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the system access authentication policy:

```
DES-3500:4#disable authen_policy
Command: disable authen_policy

Success.

DES-3500:4#
```

show authen_policy	
Purpose	Used to display the system access authentication policy status on the Switch.
Syntax	**show authen_policy**
Description	This command will show the current status of the access authentication policy on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the system access authentication policy:

```
DES-3500:4#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DES-3500:4#
```

create authen_login method_list_name

Purpose	Used to create a user defined method list of authentication methods for users logging on to the Switch.
Syntax	**create authen_login method_list_name <string 15>**
Description	This command is used to create a list for authentication techniques for user login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.
Parameters	<*string 15*> - Enter an alphanumeric string of up to 15 characters to define the given *method list*.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the method list “Trinity.”:

```
DES-3500:4#create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity

Success.

DES-3500:4#
```

config authen_login

Purpose	Used to configure a user-defined or default *method list* of authentication methods for user login.
Syntax	**config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}**
Description	This command will configure a user-defined or default *method list* of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local,* the Switch will send an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local* account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch. Successful login using any of these methods will give the user a “user”

config authen_login

privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the *enable admin* command, followed by a previously configured password. (*See the **enable admin** part of this section for more detailed information, concerning the **enable admin** command.)*

Parameters

default – The default method list for access authentication, as defined by the user. The user may choose one or a combination of up to four(4) of the following authentication methods:

- *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from the remote TACACS *server hosts* of the TACACS *server group* list.
- *xtacacs* – Adding this parameter will require the user to be authenticated using the *XTACACS* protocol from the remote XTACACS *server hosts* of the XTACACS *server group* list.
- *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list.
- *radius* - Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list.
- *server_group* <*string 15*> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.
- *local* - Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch.
- *none* – Adding this parameter will require no authentication to access the Switch.

method_list_name – Enter a previously implemented method list name defined by the user. The user may add one, or a combination of up to four (4) of the following authentication methods to this method list:

- *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from a remote TACACS server.
- *xtacacs* – Adding this parameter will require the user to be authenticated using the *XTACACS* protocol from a remote XTACACS server.
- *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from a remote TACACS+ server.
- *radius* - Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from a remote RADIUS server.
- *server_group* <*string 15*> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.
- *local* - Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch.
- *none* – Adding this parameter will require no authentication to access the Switch.

NOTE: Entering *none* or *local* as an authentication protocol will override any other authentication that follows it on a method list or on the default method list.

Restrictions

Only administrator-level users can issue this command.

Example usage:

To configure the user defined method list “Trinity” with authentication methods TACACS, XTACACS and local, in that order.

```
DES-3500:4#config authen_login method_list_name Trinity method
tacacs xtacacs local
Command: config authen_login method_list_name Trinity method tacacs
xtacacs local

Success.

DES-3500:4#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DES-3500:4#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

DES-3500:4#
```

delete authen_login method_list_name

Purpose	Used to delete a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**delete authen_login method_list_name <string 15>**
Description	This command is used to delete a list for authentication methods for user login.
Parameters	<*string 15*> - Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the method list name “Trinity”:

```
DES-3500:4#delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DES-3500:4#
```

show authen_login

Purpose	Used to display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**show authen_login [default | method_list_name <string 15> | all]**
Description	This command is used to show a list of authentication methods for user login.
Parameters	*default* – Entering this parameter will display the default method list for users logging on to the Switch.

show authen_login

	method_list_name <*string 15*> - Enter an alphanumeric string of up to 15 characters to define the given *method list* to view. *all* – Entering this parameter will display all the authentication login methods currently configured on the Switch. The window will display the following parameters: ▪ Method List Name – The name of a previously configured method list name. ▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest). ▪ Method Name – Defines which security protocols are implemented, per method list name. ▪ Comment – Defines the type of Method. *User-defined Group* refers to server group defined by the user. *Built-in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS / XTACACS / TACACS+ / RADIUS which are local (authentication through the user account on the Switch) and none (no authentication necessary to access any function on the Switch).
Restrictions	None.

Example usage:

To view the authentication login method list named Trinity:

```
DES-3500:4#show authen_login method_list_name Trinity
Command: show authen_login method_list_name Trinity

Method List Name  Priority   Method Name      Comment
----------------  --------   ---------------  ---------
Trinity           1          tacacs+          Built-in Group
                  2          tacacs           Built-in Group
                  3          Darren           User-defined Group
                  4          local            Keyword

DES-3500:4#
```

create authen_enable method_list_name

Purpose	Used to create a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**create authen_enable method_list_name <string 15>**
Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented on the Switch.
Parameters	*<string 15>* - Enter an alphanumeric string of up to 15 characters to define the given *enable method list* to create.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a user-defined method list, named "Permit" for promoting user privileges to Administrator privileges:

```
DES-3500:4#create authen_enable method_list_name Permit
Command: show authen_login method_list_name Permit

Success.

DES-3500:4#
```

config authen_enable

Purpose	Used to configure a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}**
Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented simultaneously on the Switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local_enable,* the Switch will send an authentication request to the first *TACACS* host in the server group. If no verification is found, the Switch will send an authentication request to the second *TACACS* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local_enable* password set in the Switch is used to authenticate the user. Successful authentication using any of these methods will give the user an "Admin" level privilege.
Parameters	*default* – The default method list for administration rights authentication, as defined by the user. The user may choose one or a combination of up to four (4) of the following authentication methods: ▪ *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from the remote TACACS *server hosts* of the TACACS *server group* list. ▪ *xtacacs* – Adding this parameter will require the user to be authenticated using the *XTACACS* protocol from the remote XTACACS *server hosts* of the XTACACS *server group* list. ▪ *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. ▪ *radius* – Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. ▪ *server_group <string 15>* - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. ▪ *local_enable* - Adding this parameter will require the user to

config authen_enable	
	be authenticated using the local *user account* database on the Switch. ▪ *none* – Adding this parameter will require no authentication to access the Switch. *method_list_name* – Enter a previously implemented method list name defined by the user (**create authen_enable**). The user may add one, or a combination of up to four (4) of the following authentication methods to this method list: ▪ *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from a remote TACACS server. ▪ *xtacacs* – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. ▪ *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from a remote TACACS+ server. ▪ *radius* - Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from a remote RADIUS server. ▪ *server_group <string 15>* - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. ▪ *local_enable* - Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch. The local enable password of the device can be configured using the "**config admin local_password**" command. ▪ *none* – Adding this parameter will require no authentication to access the administration level privileges on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the user defined method list "Permit" with authentication methods TACACS, XTACACS and local, in that order.

```
DES-3500:4#config authen_enable method_list_name Trinity method
tacacs xtacacs local
Command: config authen_enable method_list_name Trinity method
tacacs xtacacs local

Success.

DES-3500:4#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DES-3500:4#config authen_enable default method xtacacs tacacs+ local
Command: config authen_enable default method xtacacs tacacs+ local

Success.

DES-3500:4#
```

delete authen_enable method_list_name	
Purpose	Used to delete a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**delete authen_enable method_list_name <string 15>**
Description	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	<*string 15*> - Enter an alphanumeric string of up to 15 characters to define the given *enable method list* to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the user-defined method list "Permit"

```
DES-3500:4#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DES-3500:4#
```

show authen_enable	
Purpose	Used to display the method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**show authen_enable [default | method_list_name <string 15> | all]**
Description	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	*default* – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the Switch. *method_list_name* <*string 15*> - Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to view. all – Entering this parameter will display all the authentication login methods currently configured on the Switch. The window will display the following parameters: ▪ Method List Name – The name of a previously configured method list name. ▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest). ▪ Method Name – Defines which security protocols are implemented, per method list name. ▪ Comment – Defines the type of Method. *User-defined Group* refers to *server groups* defined by the user. *Built-in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the *local_enable* password on the Switch) and none (no authentication necessary to access any function on the Switch).
Restrictions	None.

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DES-3500:4#show authen_enable all
Command: show authen_enable all

Method List Name  Priority   Method Name  Comment
----------------  --------   -----------  ------------------
Permit            1          tacacs+      Built-in Group
                  2          tacacs       Built-in Group
                  3          Darren       User-defined Group
                  4          local        Keyword

default           1          tacacs+      Built-in Group
                  2          local        Keyword

Total Entries : 2

DES-3500:4#
```

config authen application

Purpose	Used to configure various applications on the Switch for authentication using a previously configured method list.
Syntax	**config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]**
Description	This command is used to configure Switch configuration applications (console, telnet, ssh, web) for login at the user level and at the administration level (*authen_enable*) utilizing a previously configured method list.
Parameters	*application* – Choose the application to configure. The user may choose one of the following five options to configure. ▪ *console* – Choose this parameter to configure the command line interface login method. ▪ *telnet* – Choose this parameter to configure the telnet login method. ▪ *ssh* – Choose this parameter to configure the Secure Shell login method. ▪ *http* – Choose this parameter to configure the web interface login method. ▪ *all* – Choose this parameter to configure all applications (console, telnet, ssh, web) login method. *login* – Use this parameter to configure an application for normal login on the user level, using a previously configured method list. *enable* - Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Use this parameter to configure an application for user authentication using the default method list. *method_list_name* <*string 15*> - Use this parameter to configure an application for user authentication using a previously configured method list. Enter a alphanumeric string of up to 15 characters to define a previously configured method list.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the default method list for the web interface:

```
DES-3500:4#config authen application http login default
Command: config authen application http login default

Success.

DES-3500:4#
```

show authen application

Purpose	Used to display authentication methods for the various applications on the Switch.
Syntax	**show authen application**
Description	This command will display all of the authentication method lists (login, enable administrator privileges) for Switch configuration applications (console, telnet, SSH, web) currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the login and enable method list for all applications on the Switch:

```
DES-3500:4#show authen application
Command: show authen application

Application    Login Method List   Enable Method List
-----------    -----------------   ------------------
Console        default             default
Telnet         Trinity             default
SSH            default             default
HTTP           default             default

DES-3500:4#
```

create authen server_host

Purpose	Used to create an authentication server host.
Syntax	**create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit < 1-255>}**
Description	This command will create an authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*server_host <ipaddr>* - The IP address of the remote server host to add. *protocol* – The protocol used by the server host. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol.

create authen server_host	
	▪ *xtacacs* - Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* - Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* - Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1-65535>* - Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *key <key_string 254>* - Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters. *timeout <int 1-255>* - Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* - Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a TACACS+ authentication server host, with port number 1234, a timeout value of 10 seconds and a retransmit count of 5.

```
DES-3500:4#create authen server_host 10.1.1.121 protocol tacacs+ port
1234 timeout 10 retransmit 5
Command: create authen server_host 10.1.1.121 protocol tacacs+ port
1234 timeout 10 retransmit 5

Success.

DES-3500:4#
```

config authen server_host	
Purpose	Used to configure a user-defined authentication server host.
Syntax	**create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit < 1-255>}**
Description	This command will configure a user-defined authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*server_host <ipaddr>* - The IP address of the remote server host the user wishes to alter.

config authen server_host	
	protocol – The protocol used by the server host. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* - Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* - Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ radius - Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1-65535>* - Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *key <key_string 254>* - Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters or choose none. *timeout <int 1-255>* - Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* - Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond. This field is inoperable for the TACACS+ protocol.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure a TACACS+ authentication server host, with port number 4321, a timeout value of 12 seconds and a retransmit count of 4.

```
DES-3500:4#config authen server_host 10.1.1.121 protocol tacacs+
port 4321 timeout 12 retransmit 4
Command: config authen server_host 10.1.1.121 protocol tacacs+ port
4321 timeout 12 retransmit 4

Success.

DES-3500:4#
```

delete authen server_host	
Purpose	Used to delete a user-defined authentication server host.
Syntax	**delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command is used to delete a user-defined authentication server host previously created on the Switch.
Parameters	*server_host <ipaddr>* - The IP address of the remote server host to be deleted. *protocol* – The protocol used by the server host the user wishes to delete. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* - Enter this parameter if the server host utilizes the

delete authen server_host	
	XTACACS protocol. ▪ *tacacs+* - Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* - Enter this parameter if the server host utilizes the RADIUS protocol.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a user-defined TACACS+ authentication server host:

```
DES-3500:4#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DES-3500:4#
```

show authen server_host	
Purpose	Used to view a user-defined authentication server host.
Syntax	**show authen server_host**
Description	This command is used to view user-defined authentication server hosts previously created on the Switch. The following parameters are displayed: IP Address – The IP address of the authentication server host. Protocol – The protocol used by the server host. Possible results will include TACACS, XTACACS, TACACS+ or RADIUS. Port – The virtual port number on the server host. The default value is 49. Timeout - The time in seconds the Switch will wait for the server host to reply to an authentication request. Retransmit - The value in the retransmit field denotes how many times the device will resend an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol. Key - Authentication key to be shared with a configured TACACS+ server only.
Parameters	None.
Restrictions	None.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DES-3500:4#show authen server_host
Command: show authen server_host

IP Address    Protocol   Port  Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  ----------
10.53.13.94   TACACS   49    5        2           No Use

Total Entries : 1

DES-3500:4#
```

create authen server_group	
Purpose	Used to create a user-defined authentication server group.
Syntax	**create authen server_group <string 15>**
Description	This command will create an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may add up to eight (8) authentication server hosts to this group using the **config authen server_group** command.
Parameters	<*string 15*> - Enter an alphanumeric string of up to 15 characters to define the newly created server group.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the server group "group_1":

```
DES-3500:4#create authen server_group group_1
Command: create authen server_group group_1

Success.

DES-3500:4#
```

config authen server_group	
Purpose	Used to configure a user-defined authentication server group.
Syntax	**config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command will configure an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. Up to eight (8) authentication server hosts may be added to any particular group
Parameters	*server_group* - The user may define the group by protocol groups built into the Switch (TACACS/XTACACS/TACACS+/RADIUS), or by a user-defined group previously created using the *create authen server_group* command. ▪ *tacacs* – Use this parameter to utilize the built-in TACACS server protocol on the Switch. Only server hosts utilizing the TACACS protocol may be added to this group. ▪ *xtacacs* – Use this parameter to utilize the built-in XTACACS server protocol on the Switch. Only server hosts utilizing the XTACACS protocol may be added to this group. ▪ *tacacs+* – Use this parameter to utilize the built-in TACACS+ server protocol on the Switch. Only server hosts utilizing the TACACS+ protocol may be added to this group. ▪ *radius* – Use this parameter to utilize the built-in RADIUS server protocol on the Switch. Only server hosts utilizing the RADIUS protocol may be added to this group. ▪ <*string 15*> - Enter an alphanumeric string of up to 15 characters to define the previously created server group. This group may add any combination of server hosts to it, regardless of protocol.

config authen server_group	
	add/delete – Enter the correct parameter to add or delete a server host from a server group. *server_host <ipaddr>* - Enter the IP address of the previously configured server host to add or delete. *protocol* – Enter the protocol utilized by the server host. There are three options: ▪ *tacacs* – Use this parameter to define the protocol if the server host is using the TACACS authentication protocol. ▪ *xtacacs* – Use this parameter to define the protocol if the server host is using the XTACACS authentication protocol. ▪ *tacacs+* – Use this parameter to define the protocol if the server host is using the TACACS+ authentication protocol. ▪ *radius* – Use this parameter to define the protocol if the server host is using the RADIUS authentication protocol.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add an authentication host to server group "group_1":

```
DES-3500:4# config authen server_group group_1 add server_host
10.1.1.121 protocol tacacs+
Command: config authen server_group group_1 add server_host
10.1.1.121 protocol tacacs+

Success.

DES-3500:4#
```

delete authen server_group	
Purpose	Used to delete a user-defined authentication server group.
Syntax	**delete authen server_group <string 15>**
Description	This command will delete an authentication server group.
Parameters	*<string 15>* - Enter an alphanumeric string of up to 15 characters to define the previously created server group to be deleted.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the server group "group_1":

```
DES-3500:4#delete server_group group_1
Command: delete server_group group_1

Success.

DES-3500:4#
```

show authen server_group

Purpose	Used to view authentication server groups on the Switch.
Syntax	**show authen server_group <string 15>**
Description	This command will display authentication server groups currently configured on the Switch. This command will display the following fields: Group Name: The name of the server group currently configured on the Switch, including built in groups and user defined groups. IP Address: The IP address of the server host. Protocol: The authentication protocol used by the server host.
Parameters	<*string 15*> - Enter an alphanumeric string of up to 15 characters to define the previously created server group to be viewed. Entering this command without the <*string*> parameter will display all authentication server groups on the Switch.
Restrictions	None.

Example usage:

To view authentication server groups currently set on the Switch.

```
DES-3500:4#show authen server_group
Command: show authen server_group

Group Name    IP Address                  Protocol
--------------  --------------            --------
Darren          10.53.13.2                TACACS
tacacs          10.53.13.94               TACACS
tacacs+         (This group has no entry)
xtacacs         (This group has no entry)

Total Entries : 4

DES-3500:4#
```

config authen parameter response_timeout

Purpose	Used to configure the amount of time the Switch will wait for a user to enter authentication before timing out.
Syntax	**config authen parameter response_timeout <int 0-255>**
Description	This command will set the time the Switch will wait for a response of authentication from the user.
Parameters	*response_timeout <int 0-255>* - Set the time, in seconds, the Switch will wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. 0 means there won't be a time-out. The default value is 30 seconds.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the response timeout for 60 seconds:

```
DES-3500:4# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DES-3500:4#
```

config authen parameter attempt	
Purpose	Used to configure the maximum number of times the Switch will accept authentication attempts.
Syntax	**config authen parameter attempt <int 1-255>**
Description	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet users will be disconnected from the Switch.
Parameters	*parameter attempt <int 1-255>* - Set the maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the maximum number of authentication attempts at 5:

```
DES-3500:4# config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DES-3500:4#
```

show authen parameter	
Purpose	Used to display the authentication parameters currently configured on the Switch.
Syntax	**show authen parameter**
Description	This command will display the authentication parameters currently configured on the Switch, including the response timeout and user authentication attempts. This command will display the following fields: Response timeout – The configured time allotted for the Switch to wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. User attempts: The maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.
Parameters	None.
Restrictions	None.

Example usage:

To view the authentication parameters currently set on the Switch:

```
DES-3500:4#show authen parameter
Command: show authen parameter

Response timeout : 60 seconds
User attempts    : 5

DES-3500:4#
```

enable admin	
Purpose	Used to promote user level privileges to administrator level privileges.
Syntax	**enable admin**
Description	This command is for users who have logged on to the Switch on the normal user level, to become promoted to the administrator level. After logging on to the Switch users will have only user level privileges. To gain access to administrator level privileges, the user will enter this command and will have to enter an authentication password. Possible authentication methods for this function include TACACS, XTACACS, TACACS+, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (*none*). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host which has the username "enable", and a password configured by the administrator that will support the "enable" function. This function becomes inoperable when the authentication policy is disabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable administrator privileges on the Switch:

```
DES-3500:4#enable admin
Password: ******

DES-3500:4#
```

config admin local_enable	
Purpose	Used to configure the local enable password for administrator level privileges.
Syntax	**config admin local_enable**
Description	This command will configure the locally enabled password for the **enable admin** command. When a user chooses the "*local_enable*" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is set locally on the Switch.
Parameters	*<password 15>* - After entering this command, the user will be prompted to enter the old password, then a new password in an alphanumeric string of no more than 15 characters, and finally prompted to enter the new password again for confirmation. See the example below.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the password for the "local_enable" authentication method.

```
DES-3500:4#config admin local_enable
Command: config admin local_enable

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

DES-3500:4#
```

33

SSH COMMANDS

The steps required to use the Secure Shell (SSH) protocol for secure communication between a remote PC (the SSH Client) and the Switch (the SSH Server), are as follows:

Create a user account with admin-level access using the **create account admin <username> <password>** command. This is identical to creating any other admin-lever user account on the Switch, including specifying a password. This password is used to login to the Switch, once secure communication has been established using the SSH protocol.

Configure the user account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **config ssh authmode** command. There are three choices as to the method SSH will use to authorize the user, and they are password, publickey and hostbased.

Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH Client and the SSH Server.

Finally, enable SSH on the Switch using the **enable ssh command**.

After following the above steps, users can configure an SSH Client on the remote PC and manage the Switch using secure, in-band communication.

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

Command	Parameters
enable ssh	
disable ssh	
config ssh authmode	[password | publickey | hostbased] [enable | disable]
show ssh authmode	
config ssh server	{maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]
show ssh server	
config ssh user	<username> authmode [hostbased [hostname <domain_name> | hostname_IP <domain_name> <ipaddr>] | password | publickey]
show ssh user authmode	
config ssh algorithm	[3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm	
config ssh regenerate hostkey	

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

enable shh	
Purpose	Used to enable SSH.
Syntax	**enable ssh**
Description	This command allows users to enable SSH on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Usage example:

To enable SSH:

```
DES-3500:4#enable ssh
Command: enable ssh

Success.

DES-3500:4#
```

disable ssh	
Purpose	Used to disable SSH.
Syntax	**disable ssh**
Description	This command allows users to disable SSH on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Usage example:

To disable SSH:

```
DES-3500:4# disable ssh
Command: disable ssh

Success.

DES-3500:4#
```

config ssh authmode	
Purpose	Used to configure the SSH authentication mode setting.
Syntax	**config ssh authmode [password | publickey | hostbased] [enable | disable]**
Description	This command will allow users to configure the SSH authentication mode for users attempting to access the Switch.
Parameters	*password* – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the Switch. *publickey* - This parameter may be chosen if the administrator wishes to use a publickey configuration set on a SSH server, for authentication. *hostbased* - This parameter may be chosen if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. *[enable | disable]* - This allows users to enable or disable SSH authentication on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DES-3500:4#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

DES-3500:4#
```

show ssh authmode

Purpose	Used to display the SSH authentication mode setting.
Syntax	**show ssh authmode**
Description	This command will allow users to display the current SSH authentication set on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current authentication mode set on the Switch:

```
DES-3500:4#show ssh authmode
Command: show ssh authmode

The SSH authmode:
Password      : Enabled
Publickey     : Enabled
Hostbased     : Enabled

DES-3500:4#
```

config ssh server

Purpose	Used to configure the SSH server.
Syntax	**config ssh server {maxsession <int 1-8> | timeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]**
Description	This command allows users to configure the SSH server.
Parameters	*maxsession <int 1-8>* - Allows the user to set the number of users that may simultaneously access the Switch. The default setting is 8. *contimeout <sec 120-600>* - Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default is 300 seconds. *authfail <int 2-20>* - Allows the administrator to set the maximum number of attempts that a user may try to logon utilizing SSH authentication. After the maximum number of attempts is exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. *rekey [10min | 30min | 60min | never]* - Sets the time period that the Switch will change the security shell encryptions.
Restrictions	Only administrator-level users can issue this command.

Usage example:

To configure the SSH server:

```
DES-3500:4# config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2

Success.

DES-3500:4#
```

show ssh server

Purpose	Used to display the SSH server setting.
Syntax	**show ssh server**
Description	This command allows users to display the current SSH server setting.
Parameters	None.
Restrictions	None.

Usage example:

To display the SSH server:

```
DES-3500:4# show ssh server
Command: show ssh server

The SSH server configuration
max Session              : 8
Connection timeout       : 300
Authfail attempts        : 2
Rekey timeout            : never
port                     : 22

DES-3500:4#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	**config ssh user <username 15> authmode {hostbased [hostname <domain_name> | hostname_IP <domain_name> <ipaddr>} | password | publickey]**
Description	This command allows users to configure the SSH user authentication method.
Parameters	*<username 15>* - Enter a username of no more than 15 characters to identify the SSH user. *authmode* – Specifies the authentication mode of the SSH user wishing to log on to the Switch. The administrator may choose between: • *hostbased* – This parameter should be chosen if the user wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. ◦ *hostname <domain_name>* - Enter an alphanumeric string of up to 32 characters identifying the remote SSH user. ◦ *hostname_IP <domain_name> <ipaddr>* - Enter the hostname and the corresponding IP address of the SSH user. • *password* – This parameter should be chosen to use an administrator defined password for authentication. Upon entry of

config ssh user	
	this command, the Switch will prompt the user for a password, and then to retype the password for confirmation. • *publickey* – This parameter should be chosen to use the publickey on a SSH server for authentication.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the SSH user:

```
DES-3500:4# config ssh user Trinity authmode Password
Command: config ssh user Trinity authmode Password

Enter a case sensitive new password: *******
Enter the new password again for conformation:*******

Success.

DES-3500:4#
```

show ssh user authmode	
Purpose	Used to display the SSH user setting.
Syntax	**show ssh user authmode**
Description	This command allows users to display the current SSH user setting.
Parameters	None.
Restrictions	None.

Example usage:

To display the SSH user:

```
DES-3500:4#show ssh user
Command: show ssh user

Current Accounts:
UserName              Authentication
--------------------- ---------------------
Trinity               Publickey

DES-3500:4#
```

Note: To configure the SSH user, the administrator must create a user account on the Switch. For information concerning configuring a user account, please see the section of this manual entitled **Basic Switch Commands** and then the command, **create account**.

config ssh algorithm	
Purpose	Used to configure the SSH algorithm.
Syntax	**config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]**
Description	This command allows users to configure the desired type of SSH algorithm used for authentication encryption.
Parameters	*3DES* – This parameter will enable or disable the Triple_Data Encryption Standard encryption algorithm. *AES128* - This parameter will enable or disable the Advanced Encryption Standard AES128 encryption algorithm. *AES192* - This parameter will enable or disable the Advanced Encryption Standard AES192 encryption algorithm. *AES256* - This parameter will enable or disable the Advanced Encryption Standard AES256 encryption algorithm. *arcfour* - This parameter will enable or disable the Arcfour encryption algorithm. *blowfish* - This parameter will enable or disable the Blowfish encryption algorithm. *cast128* - This parameter will enable or disable the Cast128 encryption algorithm. *twofish128* - This parameter will enable or disable the twofish128 encryption algorithm. *twofish192* - This parameter will enable or disable the twofish192 encryption algorithm. *MD5* - This parameter will enable or disable the MD5 Message Digest encryption algorithm. *SHA1* - This parameter will enable or disable the Secure Hash Algorithm encryption. *RSA* - This parameter will enable or disable the RSA encryption algorithm. *DSA* - This parameter will enable or disable the Digital Signature Algorithm encryption. *[enable | disable]* – This allows the user to enable or disable algorithms entered in this command, on the Switch.
Restrictions	Only administrator-level users can issue this command.

Usage example:

To configure SSH algorithm:

```
DES-3500:4# config ssh algorithm Blowfish enable
Command: config ssh algorithm Blowfish enable

Success.

DES-3500:4#
```

show ssh algorithm	
Purpose	Used to display the SSH algorithm setting.
Syntax	**show ssh algorithm**
Description	This command will display the current SSH algorithm setting status.
Parameters	None.
Restrictions	None.

Usage Example:

To display SSH algorithms currently set on the Switch:

```
DES-3500:4#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
3DES            :Enabled
AES128          :Enabled
AES192          :Enabled
AES256          :Enabled
ARC4            :Enabled
Blowfish        :Enabled
Cast128         :Enabled
Twofish128      :Enabled
Twofish192      :Enabled
Twofish256      :Enabled

Data Integrity Algorithm
MD5             :Enabled
SHA1            :Enabled

Public Key Algorithm
RSA             :Enabled
DSA             :Enabled

DES-3500:4#
```

config ssh regenerate hostkey

Purpose	Used to regenerate the hostkey to be recognized by the SSH server.
Syntax	**config ssh regenerate hostkey**
Description	This command is used to regenerate the hostkey to be recognized by the SSH server. Periodically, the SSH server will make a new encryption key for the host to be authorized by. Entering this command will regenerate a hostkey that will be saved into the flash memory of the Switch so a new authorization can be made with the server. Regenerating the hostkey may take several seconds.
Parameters	None.
Restrictions	None.

Example usage:

To regenerate the hostkey to be used by the Switch for authorization with the server.

```
DES-3500:4#config ssh regenerate hostkey
Command: config ssh regenerate hostkey

Success.

DES-3500:4#
```

34

SSL COMMANDS

Secure Sockets Layer or ***SSL*** is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a *ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the cyphersuite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE_DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
   - **Stream Ciphers** – There are two types of stream ciphers on the Switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
   - **CBC Block Ciphers** – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES_EDE encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.
3. **Hash Algorithm**: This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

Command	Parameters
enable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
config ssl cachetimeout timeout	<value 60-86400>
show ssl	
show ssl certificate	
show ssl cachetimeout	
download certificate_fromTFTP	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

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

enable ssl	
Purpose	To enable the SSL function on the Switch.
Syntax	**enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}**
Description	This command will enable SSL on the Switch by implementing any one or combination of listed ciphersuites on the Switch. Entering this command without a parameter will enable the SSL status on the Switch. Enabling SSL will disable the web-manager on the Switch.
Parameters	*ciphersuite* - A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: • *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. • *RSA_with_3DES_EDE_CBC_SHA* - This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. • *DHE_DSS_with_3DES_EDE_CBC_SHA* - This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. • *RSA_EXPORT_with_RC4_40_MD5* - This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys. The ciphersuites are enabled by default on the Switch, yet the SSL status is disabled by default. Enabling SSL with a ciphersuite will not enable the SSL status on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DES-3500:4#enable ssl
Command: enable ssl

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

DES-3500:4#
```

NOTE: Enabling SSL on the Switch will enable all ciphersuites. To utilize a particular ciphersuite, the user must eliminate other ciphersuites by using the **disable ssl** command along with the appropriate ciphersuites.

NOTE: Enabling the SSL function on the Switch will disable the port for the web manager (port 80). To log on to the web based manager, the entry of the URL must begin with *https://*. (ex. https://10.90.90.90)

disable ssl

Purpose	To disable the SSL function on the Switch.
Syntax	**disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}**
Description	This command will disable SSL on the Switch and can be used to disable any one or combination of listed ciphersuites on the Switch.
Parameters	*ciphersuite* - A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: • *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. • *RSA_with_3DES_EDE_CBC_SHA* - This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. • *DHE_DSS_with_3DES_EDE_CBC_SHA* - This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. • *RSA_EXPORT_with_RC4_40_MD5* - This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DES-3500:4#disable ssl
Command: disable ssl

Success.

DES-3500:4#
```

To disable ciphersuite *RSA_EXPORT_with_RC4_40_MD5* only:

```
DES-3500:4#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5

Success.

DES-3500:4#
```

config ssl cachetimeout timeout

Purpose	Used to configure the SSL cache timeout.
Syntax	**config ssl cachetimeout timeout <value 60-86400>**
Description	This command will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process.

config ssl cachetimeout timeout	
Parameters	*timeout* <*value 60-86400*> - Enter a timeout value between *60* and *86400* seconds to specify the total time an SSL key exchange ID stays valid before the SSL module will require a new, full SSL negotiation for connection. The default cache timeout is 600 seconds
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the SSL cachetimeout for 7200 seconds:

```
DES-3500:4#config ssl cachetimeout timeout 7200
Command: config ssl cachetimeout timeout 7200

Success.

DES-3500:4#
```

show ssl cachetimeout	
Purpose	Used to show the SSL cache timeout.
Syntax	**show ssl cachetimeout**
Description	Entering this command will allow the user to view the SSL cache timeout currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL cache timeout on the Switch:

```
DES-3500:4#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DES-3500:4#
```

show ssl	
Purpose	Used to view the SSL status and the certificate file status on the Switch.
Syntax	**show ssl**
Description	This command is used to view the SSL status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DES-3500:4#show ssl
Command: show ssl

 SSL status                                Disabled
 RSA_WITH_RC4_128_MD5              0x0004  Enabled
 RSA_WITH_3DES_EDE_CBC_SHA         0x000A  Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA     0x0013  Enabled
 RSA_EXPORT_WITH_RC4_40_MD5        0x0003  Enabled


DES-3500:4#
```

show ssl certificate

Purpose	Used to view the SSL certificate file status on the Switch.
Syntax	**show ssl certificate**
Description	This command is used to view the SSL certificate file information currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view certificate file information on the Switch:

```
DES-3500:4# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DES-3500:4#
```

download certificate_fromTFTP

Purpose	Used to download a certificate file for the SSL function on the Switch.
Syntax	**download certificate_fromTFTP <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>**
Description	This command is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions.
Parameters	*<ipaddr>* - Enter the IP address of the TFTP server. *certfilename <path_filename 64>* - Enter the path and the filename of the certificate file users wish to download. *keyfilename <path_filename 64>* - Enter the path and the filename of the key exchange file users wish to download.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To download a certificate file and key file to the Switch:

DES-3500:4# DES-3500:4#download certificate_fromTFTP 10.53.13.94 certfilename c:/cert.der keyfilename c:/pkey.der

Command: download certificate_fromTFTP 10.53.13.94 certfilename c:/cert.der keyfilename c:/pkey.der

Certificate Loaded Successfully!

DES-3500:4#

35

D-LINK SINGLE IP MANAGEMENT COMMANDS

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

SIM is an optional feature on the Switch and can easily be enabled or disabled. SIM grouping has no effect on the normal operation of the Switch in the user's network.

There are three classifications for switches using SIM. The **Commander Switch(CS)**, which is the master switch of the group, **Member Switch(MS)**, which is a switch that is recognized by the CS a member of a SIM group, and a **Candidate Switch(CaS)**, which is a switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

A SIM group can only have one Commander Switch(CS).

All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

A SIM group accepts up to 32 switches (numbered 0-31), including the Commander Switch (numbered 0).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.

SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DES-3500 may take on three different roles:

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

- It has an IP Address.
- It is not a Commander Switch or Member Switch of another Single IP group.
- It is connected to the Member Switches through its management VLAN.

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

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

Candidate Switch(CaS) – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group through an automatic function of the DES-3500, or by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

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

The following rules also apply to the above roles:

1. Each device begins in the Commander state.
2. CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus the CS cannot directly be converted to a MS.
3. The user can manually configure a CS to become a CaS.
4. A MS can become a CaS by:
   a. Being configured as a CaS through the CS.
   b. If report packets from the CS to the MS time out.
5. The user can manually configure a CaS to become a CS
6. The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DES-3500 switches may join the group by either an automatic method or by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

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

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

The Upgrade to v1.6

To better improve SIM management, the xStack DES-3500 series switches have been upgraded to version 1.6 in this release. Many improvements have been made, including:

The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintain packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches. There are some instances where pre-saved MS switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

This version will support multiple switch upload and downloads for firmware, configuration files and log files, as follows:

- Firmware – The switch now supports multiple MS firmware downloads from a TFTP server.
- Configuration Files – This switch now supports multiple downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server..
- Log – The switch now supports uploading multiple MS log files to a TFTP server.

NOTE: For more details regarding improvements made in SIMv1.6, please refer to the White Paper located on the D-Link website.

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

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

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

enable sim	
Purpose	Used to enable Single IP Management (SIM) on the Switch
Syntax	**enable sim**
Description	This command will enable SIM globally on the Switch. SIM features and functions will not function properly unless this function is enabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable SIM on the Switch:

```
DES-3500:4#enable sim
Command: enable sim

Success.

DES-3500:4#
```

disable sim	
Purpose	Used to disable Single IP Management (SIM) on the Switch
Syntax	**disable sim**
Description	This command will disable SIM globally on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable SIM on the Switch:

```
DES-3500:4#disable sim
Command: disable sim

Success.

DES-3500:4#
```

show sim	
Purpose	Used to view the current information regarding the SIM group on the Switch.
Syntax	**show sim {[candidates {<candidate_id 1-32>} | members {<member_id 1-32>} | group {commander_mac <macaddr>}] | neighbor]}**
Description	This command will display the current information regarding the SIM group on the Switch, including the following: SIM Version - Displays the current Single IP Management version on

show sim	
	the Switch. Firmware Version - Displays the current Firmware version on the Switch. Device Name - Displays the user-defined device name on the Switch. MAC Address - Displays the MAC Address of the Switch. Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3). Platform – Switch Description including name and model number. SIM State –Displays the current Single IP Management State of the Switch, whether it be enabled or disabled. Role State – Displays the current role the Switch is taking, including Commander, Member or Candidate. A Stand-alone switch will always have the commander role. Discovery Interval - Time in seconds the Switch will send discovery packets out over the network. Hold time – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.
Parameters	*candidates <candidate_id 1-32>* - Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's ID number, listed from 1 to 32. *members <member_id 1-32>* - Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's id number, listed from 1 to 32. *group {commander_mac <macaddr>}* - Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group. *neighbor* – Entering this parameter will display neighboring devices of the Switch. A SIM neighbor is defined as a switch that is physically connected to the Switch but is not part of the SIM group. This screen will produce the following results: Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located. MAC Address – Displays the MAC Address of the neighbor switch. Role – Displays the role(CS, CaS, MS) of the neighbor switch.
Restrictions	None.

Example usage:

To show the SIM information in detail:

```
DES-3500:4#show sim
Command: show sim

SIM Version          : VER-1.61
Firmware Version     : Build 4.01-B19
Device Name          :
MAC Address          : 00-35-26-11-11-00
Capabilities         : L2
Platform             : DES-3526 L2 Switch
SIM State            : Enabled
Role State           : Commander
Discovery Interval   : 60 sec
Hold Time            : 180 sec

DES-3500:4#
```

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

```
DES-3500:4#show sim candidates
Command: show sim candidates

ID   MAC Address         Platform /              Hold    Firmware     Device Name
                         Capability              Time    Version
---  ----------------    ----------------------  -----   ---------    ----------------
1    00-01-02-03-04-00   DES-3526 L2 Switch      40      4.01-B19     The Man
2    00-55-55-00-55-00   DES-3526 L2 Switch      140     4.01-B19     default master

Total Entries: 2

DES-3500:4#
```

To show the member information in summary:

```
DES-3500:4#show sim member
Command: show sim member

ID   MAC Address         Platform /              Hold    Firmware     Device Name
                         Capability              Time    Version
---  ----------------    ----------------------  ----    ---------    ----------------
1    00-01-02-03-04-00   DES-3526 L2 Switch      40      4.01-B19     The Man
2    00-55-55-00-55-00   DES-3526 L2 Switch      140     4.01-B19     default master

Total Entries: 2

DES-3500:4#
```

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

```
DES-3500:4#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address         Platform /              Hold    Firmware     Device Name
                        Capability              Time    Version
--- ----------------    ----------------------  -----   ---------    ----------------
*1  00-01-02-03-04-00   DES-3526 L2 Switch      40      4.01-B19     Trinity
 2  00-55-55-00-55-00   DES-3526 L2 Switch      140     4.01-B19     default master

SIM Group Name : SIM2

ID  MAC Address         Platform /              Hold    Firmware     Device Name
                        Capability              Time    Version
--- ----------------    ----------------------  ------  ---------    ----------------
*1  00-01-02-03-04-00   DES-3526 L2 Switch      40      4.01-B19     Neo
 2  00-55-55-00-55-00   DES-3526 L2 Switch      140     4.01-B19     default master

'*' means commander switch.

DES-3500:4#
```

Example usage:

To view SIM neighbors:

```
DES-3500:4#show sim neighbor
Command: show sim neighbor

Neighbor Info Table
```

```
Port    MAC Address        Role
------  -----------------  ---------
23      00-35-26-00-11-99  Commander
23      00-35-26-00-11-91  Member
24      00-35-26-00-11-90  Candidate

Total Entries: 3

DES-3500:4#
```

reconfig	
Purpose	Used to connect to a member switch, through the commander switch, using Telnet.
Syntax	**reconfig {member_id <value 1-32 | exit}**
Description	This command is used to reconnect to a member switch using Telnet.
Parameters	*member_id* <*value 1-32*> - Select the ID number of the member switch to configure. *exit* – This command is used to exit from managing the member switch and will return to managing the commander switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To connect to the MS, with member ID 2, through the CS, using the command line interface:

```
DES-3500:4#reconfig  member_id 2
Command: reconfig  member_id 2

DES-3500:4#
Login:
```

config sim_group	
Purpose	Used to add candidates and delete members from the SIM group.
Syntax	**config sim [add <candidate_id 1-32> {<password>} | delete <member_id 1-32>]**
Description	This command is used to add candidates and delete members from the SIM group by ID number.
Parameters	*add* <*candidate_id*> <*password*> - Use this parameter to change a candidate switch (CaS) to a member switch (MS) of a SIM group. The CaS may be defined by its ID number and a password (if necessary). *delete* <*member_id 1-32*> - Use this parameter to delete a member switch of a SIM group. The member switch should be defined by ID number.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add a member:

```
DES-3500:4#config sim_group add 2
Command: config sim_group add 2

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

Success.

DES-3500:4#
```

To delete a member:

```
DES-3500:4# config sim delete 1
Command: config sim delete 1

Please wait for ACK...
Success.

DES-3500:4#
```

config sim

Purpose	Used to configure role parameters for the SIM protocol on the Switch.
Syntax	**config sim [{[commander {group_name <groupname 64> | candidate] | dp_interval <30-90> | hold_time <sec 100-255>}]**
Description	This command is used to configure parameters of switches of the SIM.
Parameters	*commander* – Use this parameter to configure the commander switch (CS) for the following parameters: ▪ *group_name <groupname 64>* - Used to update the name of the group. Enter an alphanumeric string of up to 64 characters to rename the SIM group. ▪ *dp_interval <30-90>* – The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to the CS will include information about other switches connected to it. (Ex. MS, CaS). The user may set the *dp_interval* from 30 to 90 seconds. ▪ *hold time <sec 100-300>* – Using this parameter, the user may set the time, in seconds, the CS will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 300 seconds. *candidate* – Used to change the role of a CS (commander) to a CaS (candidate). ▪ *dp_interval <30-90>* – The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to the CS will include information about other switches connected to it. (Ex. MS, CaS). The user may set the *dp_interval* from 30 to 90 seconds. ▪ *hold time <100-255>* – Using this parameter, the user may set the time, in seconds, the Switch will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 255 seconds.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To change the time interval of the discovery protocol:

```
DES-3500:4# config sim commander dp_interval 30
Command: config sim commander dp_interval 30

Success.

DES-3500:4#
```

To change the hold time of the discovery protocol:

```
DES-3500:4# config sim commander hold_time 120
Command: config sim commander hold_time 120

Success.

DES-3500:4#
```

To transfer the CS (commander) to be a CaS (candidate):

```
DES-3500:4# config sim_role candidate
Command: config sim_role candidate

Success.

DES-3500:4#
```

To transfer the Switch to be a CS:

```
DES-3500:4# config sim commander
Command: config sim commander

Success.

DES-3500:4#
```

To update the name of a group:

```
DES-3500:4# config sim commander group_name Trinity
Command: config sim commander group_name Trinity

Success.

DES-3500:4#
```

download sim

Purpose	Used to download firmware or configuration file to an indicated device.
Syntax	**download sim [firmware | configuration] <ipaddr> <path_filename> {members <mslist> | all}**
Description	This command will download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	*firmware* – Specify this parameter to download firmware to members of a SIM group. *configuration* - Specify this parameter to download a switch configuration to members of a SIM group. <*ipaddr*> – Enter the IP address of the TFTP server. <*path_filename*> – Enter the path and the filename of the firmware or switch on the TFTP server. *members* – Enter this parameter to specify the members to which the user prefers to download firmware or switch configuration files. The user may specify a member or members by adding one of the following: ▪ <*mslist*> - Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration. ▪ *all* – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To download firmware:

```
DES-3500:4# download sim firmware 10.53.13.94 c:/des3526.had members all
Command: download sim firmware 10.53.13.94 c:/des3526.had members all

This device is updating firmware.  Please wait...

Download Status :

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

DES-3500:4#
```

To download configuration files:

```
DES-3500:4# download sim configuration 10.53.13.94 c:/des3526.txt members all
Command: download sim firmware 10.53.13.94 c:/des3526.txt members all

This device is updating configuration.  Please wait...

Download Status :

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

DES-3500:4#
```

upload sim_ms

Purpose	User to upload a configuration file to a TFTP server from a specified member of a SIM group.
Syntax	**upload sim_ms <ipaddr> <path_filename> <member_id 1-32>**
Description	This command will upload a configuration file to a TFTP server from a specified member of a SIM group.
Parameters	*<ipaddr>* - Enter the IP address of the TFTP server to which to upload a configuration file. *<path_filename>* – Enter a user-defined path and file name on the TFTP server to which to upload configuration files. *<member_id 1-32>* - Enter this parameter to specify the member to which to upload a switch configuration file. The user may specify a member or members by adding the ID number of the specified member.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DES-3500:4# upload sim_ms configuration 10.55.47.1
D:\configuration.txt 1
Command: upload sim_ms configuration 10.55.47.1
D:\configuration.txt 1

Success.

DES-3500:4#
```

36

COMMAND HISTORY LIST

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

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

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

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	**? {<command>}**
Description	This command will display all of the commands available through the Command Line Interface (CLI).
Parameters	*{<command>}* – Entering the question mark with an appropriate command will list all the corresponding parameters for the specified command, along with a brief description of the commands function and similar commands having the same words in the command.
Restrictions	None.

Example usage

To display all of the commands in the CLI:

```
DES-3500:4#?
..
?
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
```

To display the parameters for a specific command:

```
DES-3500:4# config stp
Command:? config stp

Command: config stp
Usage: {maxage <value 6-40> | maxhops <value1-20> | hellotime <value 1-
10> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable |
disable] | lbd [enable | disable] | lbd_recover_timer [0 | <value 60-1000000>]}
Description: Used to update the STP Global Configuration.
config stp instance_id
config stp mst_config_id
config stp mst_ports
config stp ports
config stp priority
config stp version

DES-3500:4#
```

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

Example usage:

To display all commands:

```
DES-3500:4#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-3500:4#config command_history 20
Command: config command_history 20

Success.

DES-3500:4#
```

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-3500:4#show command_history
Command: show command_history

?
? show
show vlan
show command history

DES-3500:4#
```

A

TECHNICAL SPECIFICATIONS

General	
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP "Mini GBIC") IEEE 802.1D Spanning Tree IEEE 802.1W Rapid Spanning Tree IEEE 802.1S Multiple 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:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
Fiber Optic	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)
Topology	Star
Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)

Physical and Environmental		
Internal power supply	DES-3526 DES-3526 DC 60W	AC Input: 100 – 120; 200 – 240 VAC, 50/60 Hz DC Power Input: 48 V Output: 12V
Power Consumption	23 watts maximum	
DC fans:	one 40 mm fan	
Operating Temperature	0 - 40°C	
Storage Temperature	-40 - 70°C	
Humidity	5 - 95% non-condensing	
Dimensions	441 mm 207 mm 44 mm (1U), 19 inch rack-mount width	
Weight	DES-3526 2.56 kg / DES-3526DC 2.5 kg	
EMI	CE class A, FCC Class A, C-Tick, VCCI Class A	
Safety	CSA International	

Performance	
Transmission Method	Store-and-forward
Packet Buffer	16 MB per device
Packet Filtering / Forwarding Rate	Full-wire speed for all connections. 1,488,095 pps per port (for 1000Mbps)
MAC Address Learning	Automatic update. Supports 8K MAC address.
Priority Queues	4 Priority Queues per port.
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.