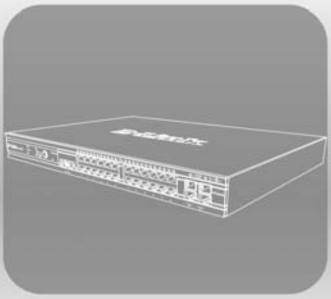
D-Link®
Building Networks for People



XSTACK

CLI Manual

Product Model: xStack™ DES-3800 Series

Layer 3 Stackable Fast Ethernet Managed Switch

Release 4.5

D-Link®

July 2008

651ES3800055G

♻

RECYCLABLE

Table of Contents

1

INTRODUCTION

The DES-3800 series is a member of the D-Link xStack switch family. xStack is a complete family of stackable devices that ranges from edge 10/100Mbps switches to core Gigabit switches. xStack provides unsurpassed performance, fault tolerance, scalable flexibility, robust security, standard-based interoperability and an impressive support for 10Gigabit technology to future-proof departmental and enterprise network deployments with an easy migration path.

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

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

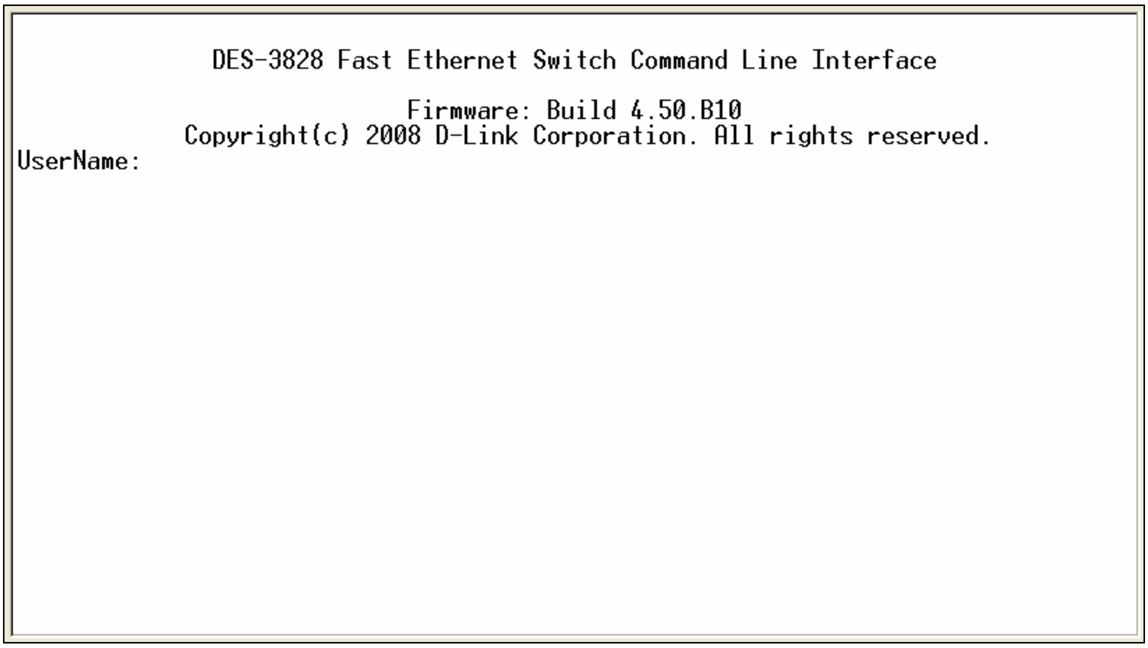
Accessing the Switch via the Serial Port

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

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

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 o refresh the console screen.



```
               DES-3828 Fast Ethernet Switch Command Line Interface

                              Firmware: Build 4.50.B10
              Copyright(c) 2008 D-Link Corporation. All rights reserved.
UserName:
```

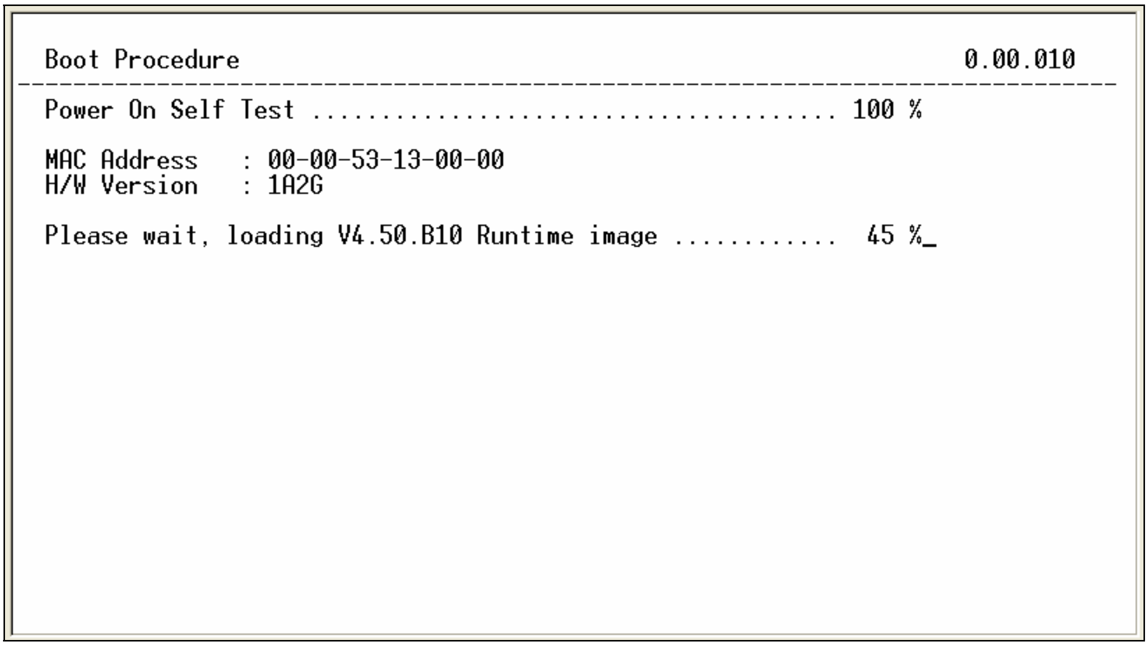
Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-3800:admin#**. This is the command line where all commands are input.

Setting the Switch's IP Address

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

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



```
 Boot Procedure                                                    0.00.010
-------------------------------------------------------------------------------
 Power On Self Test ...................................... 100 %

 MAC Address    : 00-00-53-13-00-00
 H/W Version    : 1A2G

 Please wait, loading V4.50.B10 Runtime image ...........  45 %_
```

Figure 1-2. Boot Screen

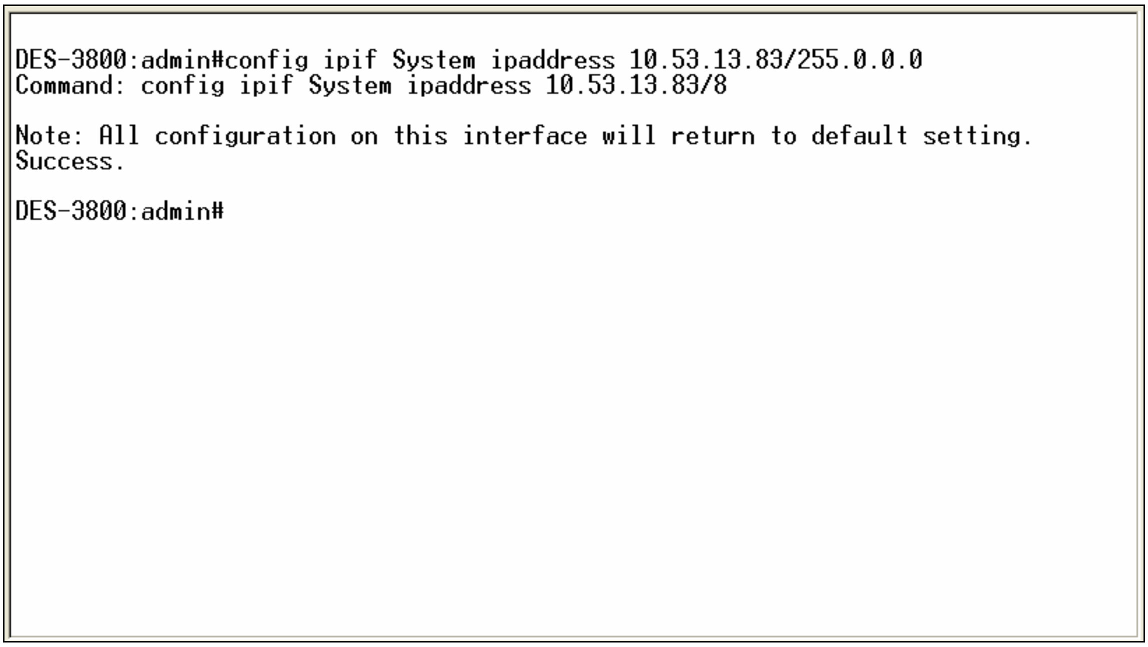
The Switch's MAC address can also be found in the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.

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

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

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

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



```
DES-3800:admin#config ipif System ipaddress 10.53.13.83/255.0.0.0
Command: config ipif System ipaddress 10.53.13.83/8

Note: All configuration on this interface will return to default setting.
Success.

DES-3800:admin#
```

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.53.13.83 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 Switch supports a console management interface that allows the user to connect to the Switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the Switch to use an SNMP-based network management software over the network.

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

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

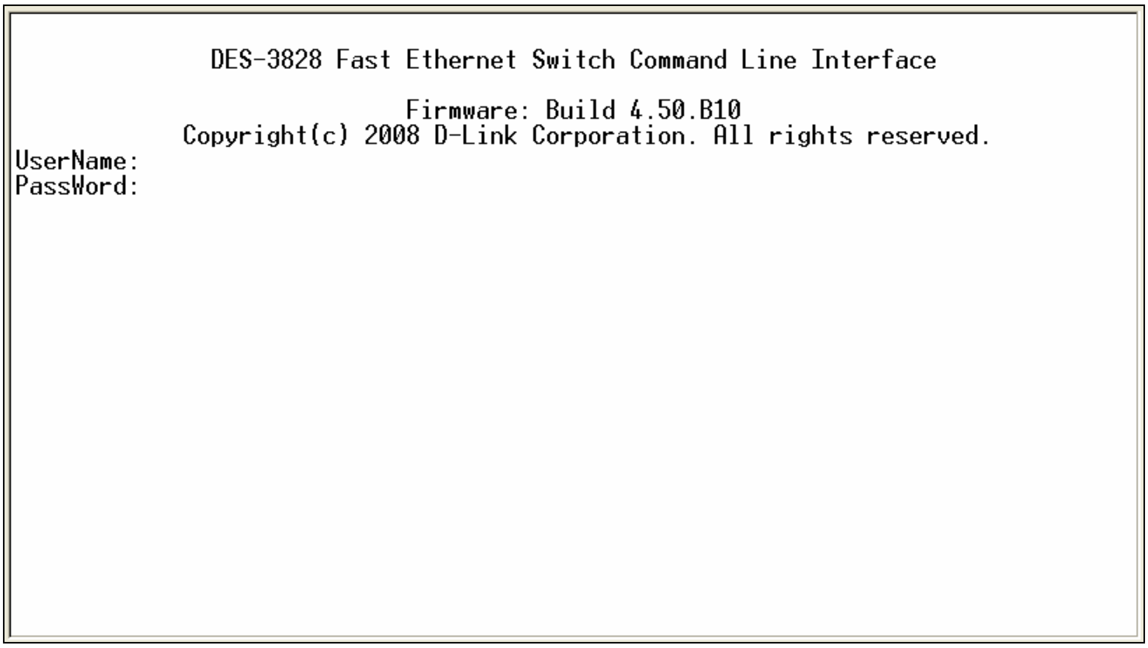
Connecting to the Switch

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

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

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

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

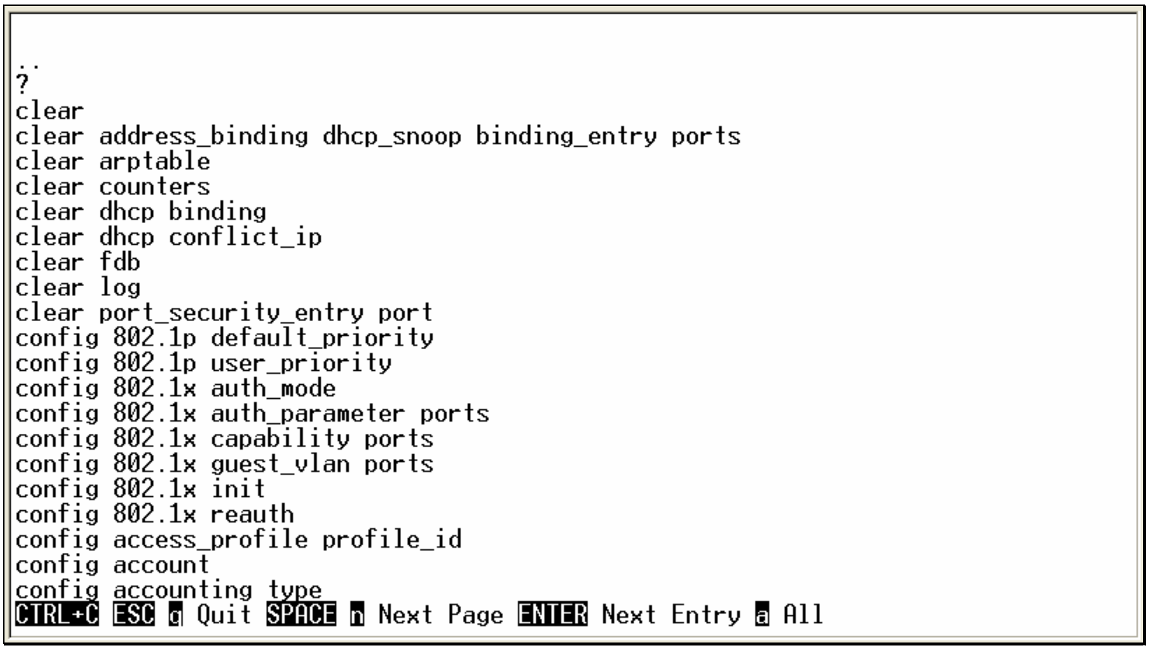


```
               DES-3828 Fast Ethernet Switch Command Line Interface

                            Firmware: Build 4.50.B10
            Copyright(c) 2008 D-Link Corporation. All rights reserved.
UserName:
PassWord:
```

Figure 2- 1. Initial Console Screen after logging in

Commands are entered at the command prompt, **DES-3800:admin#**.

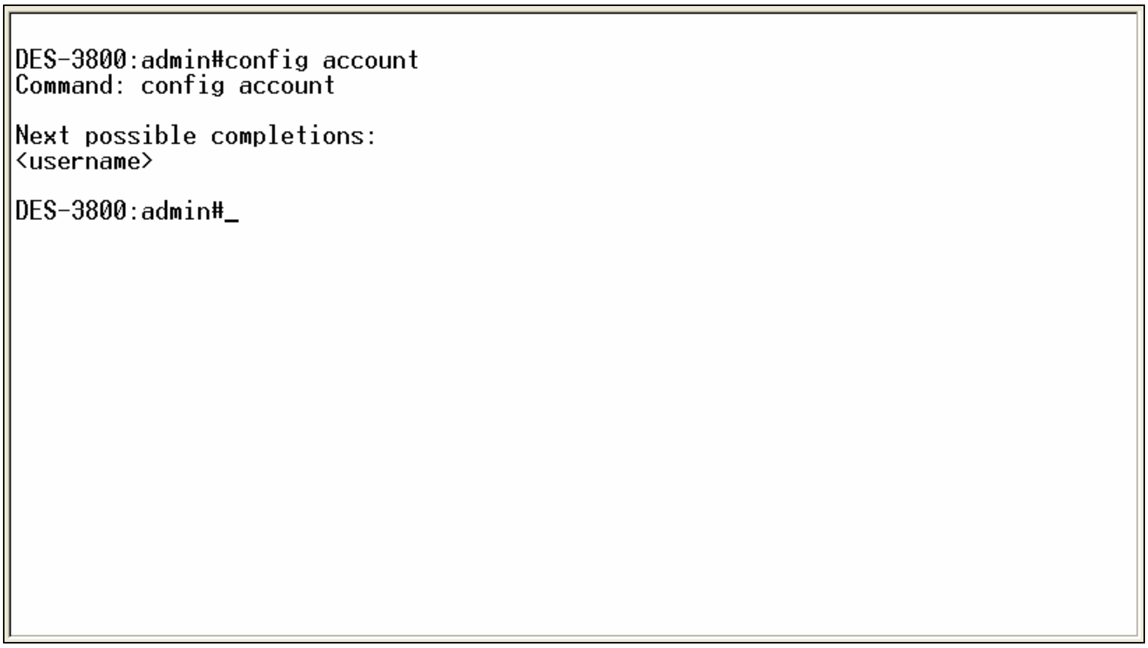
There are a number of helpful features included in the CLI. Entering the **?** command will display a list of all of the top-level commands.



```
..
?
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear dhcp binding
clear dhcp conflict_ip
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 capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config accounting type
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Figure 2- 2. The ? Command

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



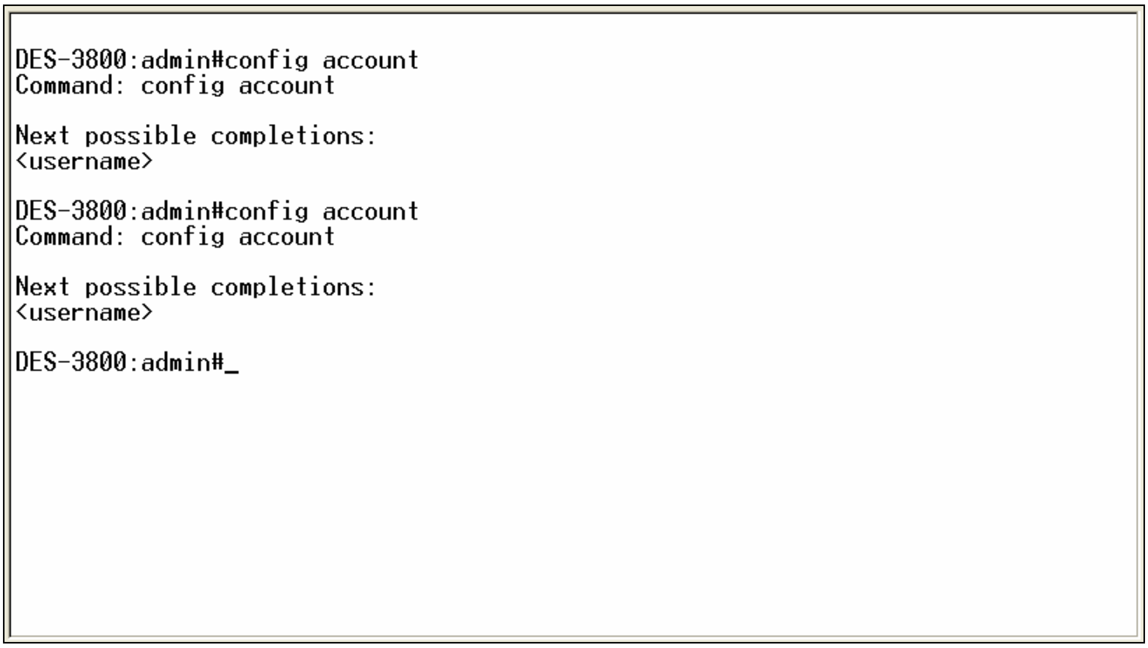
```
DES-3800:admin#config account
Command: config account

Next possible completions:
<username>

DES-3800:admin#_
```

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 you to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

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

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



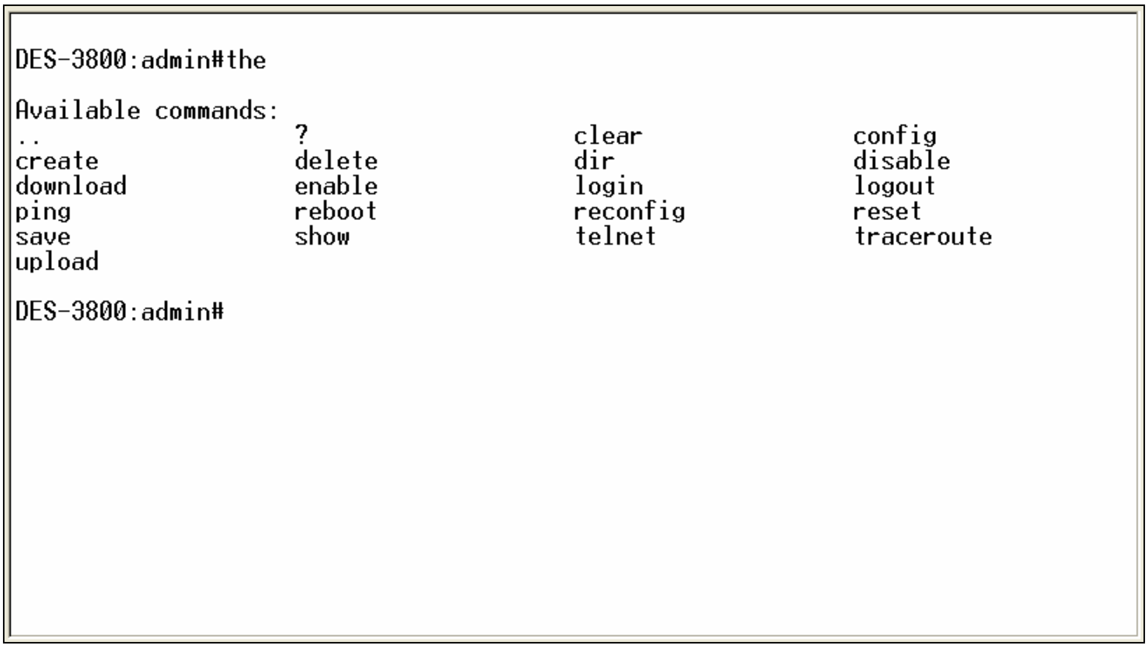
```
DES-3800:admin#config account
Command: config account

Next possible completions:
<username>

DES-3800:admin#config account
Command: config account

Next possible completions:
<username>

DES-3800:admin#_
```

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

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

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

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

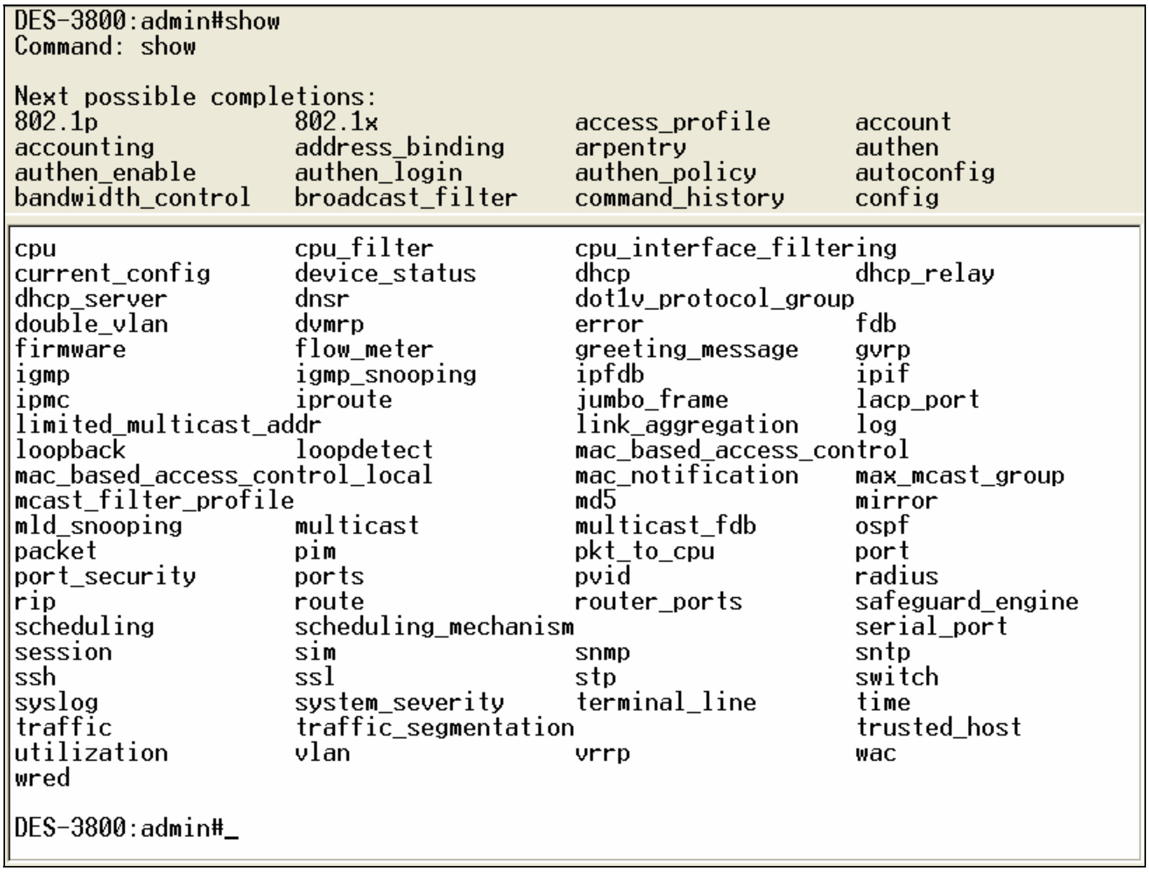


```
DES-3800:admin#the

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

DES-3800:admin#
```

Figure 2- 5. Available Commands

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

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



```
DES-3800:admin#show
Command: show

Next possible completions:
802.1p              802.1x              access_profile      account
accounting          address_binding     arpentry            authen
authen_enable       authen_login        authen_policy       autoconfig
bandwidth_control   broadcast_filter    command_history     config

cpu                 cpu_filter          cpu_interface_filtering
current_config      device_status       dhcp                dhcp_relay
dhcp_server         dnsr                dot1v_protocol_group
double_vlan         dvmrp               error               fdb
firmware            flow_meter          greeting_message    gvrp
igmp                igmp_snooping       ipfdb               ipif
ipmc                iproute             jumbo_frame         lacp_port
limited_multicast_addr                  link_aggregation    log
loopback            loopdetect          mac_based_access_control
mac_based_access_control_local          mac_notification    max_mcast_group
mcast_filter_profile                    md5                 mirror
mld_snooping        multicast           multicast_fdb       ospf
packet              pim                 pkt_to_cpu          port
port_security       ports               pvid                radius
rip                 route               router_ports        safeguard_engine
scheduling          scheduling_mechanism                    serial_port
session             sim                 snmp                sntp
ssh                 ssl                 stp                 switch
syslog              system_severity     terminal_line       time
traffic             traffic_segmentation                    trusted_host
utilization         vlan                vrrp                wac
wred

DES-3800:admin#_
```

Figure 2- 6. Next possible completions: Show Command

In the above example, all of the possible next parameters for the **show** command are displayed.

3

COMMAND SYNTAX

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

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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**create ipif <ipif_name 12> <network_address> (<ip_addr/netmask>) <vlan_name 32> {secondary | state [enable | disable]} | proxy_arp [enable | disable]}**
Description	In the above syntax example, you must supply an IP interface name in the <ipif_name> space, a VLAN name in the <vlan_name 32> space, and the network address, including the netmask, in the <network_address> (<ip_addr/netmask>) space. Do not type the angle brackets.
Example Command	**create ipif Engineering 10.24.22.5/255.0.0.0 Design**

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	**create account [admin | operator | user] <username 15>**
Description	In the above syntax example, you must specify either an **admin, operator** 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 | operator | user] <username 15>**
Description	In the above syntax example, you must specify either **admin, operator** 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, you have the option to specify **config** or **detail**. It is not necessary to specify either optional value, however the effect of the system reset is dependent on which, if any, value is specified. Therefore, with this example there are three possible outcomes of performing a system reset. See the following chapter, Basic Commands for more details about the reset command.
Example command	**reset config**

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

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

4

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin | operator | user] <username 15>
config account	<username>
show account	
delete account	<username>
show session	
show switch	
show serial_port	
config serial_port	baud_rate [9600 | 19200 | 38400 | 115200] auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>
disable web	
enable snmp	
disable snmp	
save	config <config_id1-2>
reboot	
reset	[config | system]
login	
logout	
show config	[current_config | config_in_nvram <config_ id 1-2> | information]
config configuration	<config_id 1-2> [active | delete | boot_up]
telnet	<ipaddr> {tcp_port <value 0-65535>}
config terminal line	
show terminal line	

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

create account

Purpose	Used to create user accounts.
Syntax	**create account [admin | operator | 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	The administrator can choose one of the following three levels of privileges available on the Switch. *admin* – Select this parameter to create an administrator-level account for the Switch. *admin* accounts have access and configuration rights to all components of the software of the Switch. Switch administrators must first create an admin-level account before an operator or user account can be created. Only admin level users can create other user accounts. *operator* – Select this parameter to create a operator-level user account for the Switch. Operator-level users will have rights to switch configurations, network monitoring commands, community strings and trap stations, and system utilities. All security commands, user account commands and the factory reset command will be denied from this privilege level. *user* – Select this parameter to create a user-level account on the Switch. User-level accounts have read-only rights to configuration commands, network monitoring commands and commands for community stations and trap strings. • *<username 15>* - Enter a username of no more than 15 alphanumeric characters to identify the account created here.
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-3800:admin#create account admin dlink
Command: create account admin dlink

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

Success.

DES-3800:admin#
```

To create an operator-level user account with the username “oper”.

```
DES-3800:admin#create account operator oper
Command: create account operator oper

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

Success.

DES-3800:admin#
```

To create an user-level user account with the username “system”.

```
DES-3800:admin#create account user system
Command: create account user system

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

Success.

DES-3800:admin#
```

The following table summarizes the Admin, Operator and User privileges:

Management	Admin	Operator	User
Configuration	Yes	Yes	Read-only
Network Monitoring	Yes	Yes	Read-only
Community Strings and Trap Stations	Yes	Yes	Read-only
Update Firmware and Configuration Files	Yes	No	No
System Utilities	Yes	Yes	No
Factory Reset	Yes	No	No
User Account Management			
Add/Update/Delete User Accounts	Yes	No	No
View User Accounts	Yes	No	No

NOTE: One admin-level account must be created before other user accounts can be set. When a user logs in to the Switch, the default command prompt will display the level of privilege assigned. (DES-3800:admin#, DES-3800:oper#, DES-3800:user#). For more information regarding user accounts, see the ***DES-3800 Series Layer 3 Stackable Fast Ethernet Managed Switch User Manual***.

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* > - Name of the account. The account must already be defined.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user password of “dlink” account:

```
DES-3800:admin#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-3800:admin#
```

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-3800:admin#show account
Command: show account

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

Total Entries: 1

DES-3800:admin#
```

delete account

Purpose	Used to delete an existing account.
Syntax	delete account <username> {force_agree}
Description	The delete account command deletes an existing account.
Parameters	*<username>* - Name of the user who will be deleted. *force_agree* - When force_agree is specified, the delete account command will be executed immediatedly without further confirmation.
Restrictions	Only Administrator-level users can issue this command. One active admininstrator-level user must exist.

Example usage:

To delete the user account “System”:

```
DES-3800:admin#delete account System
Command: delete account System

Success.

DES-3800:admin#
```

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	Only Administrator or Operator-level users can issue this command.

Example usage:

To display the way that the users are logged in:

```
DES-3800:admin# show session
Command: show session

ID  Login Time           Live Time    From          Level  Name
--  -------------------  -----------  ------------  -----  ----------
*0  2008/06/19 09:15:00  0:4:45.300   10.11.22.33   5      Anonymous
 8


DES-3800:admin#
```

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	None.

Example usage:

To display the Switch's information:

```
DES-3800:admin#show switch
Command: show switch

Device Type       : DES-3800 Fast-Ethernet Switch
Combo Port Type   : 1000Base-TX + 1000Base-TX
MAC Address       : 00-00-53-13-00-00
IP Address        : 10.9.68.90 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 0.00.010
Firmware Version  : Build 4.50.B10
Hardware Version  : A2
Serial Number     : N/A
Power Status      : Main - Abnormal, Redundant - Not Present
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Enabled
GVRP              : Disabled
IGMP Snooping     : Disabled
TELNET            : Enabled (TCP 23)
SSH               : Enabled (TCP 22)
WEB               : Enabled (TCP 80)
RMON              : Disabled
RIP               : Disabled
DVMRP             : Disabled
PIM               : Disabled
OSPF              : Disabled
SNMP              : Disabled

DES-3800:admin#
```

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-3800:admin#show serial_port
Command: show serial_port

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

DES-3800:admin#
```

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. *auto_logout [never | 2_minutes | 5_minutes |10_minutes | 15_minutes*
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure baud rate:

```
DES-3800:admin#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DES-3800:admin#
```

enable clipaging	
Purpose	Used to enable the feature that pauses the scrolling of the console screen when the show command displays more than one page.
Syntax	**enable clipaging**
Description	This command enables the screen to be paused when the **show command** output reaches the end of the page. The default setting is *enable*.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the feature that allows the screen to be paused when the **show command** output reaches the end of the page:

```
DES-3800:admin#enable clipaging
Command: enable clipaging


Success.
```

```
DES-3800:admin#
```

disable clipaging

Purpose	Used to disable the feature that pauses the scrolling of the console screen when the show command displays more than one page.
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 displays more than one screen of information.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#disable clipaging
Command: disable clipaging

Success.

DES-3800:admin#
```

enable telnet

Purpose	This feature enables the Switch to be managed via TELNET based management software and also allows you to specify the port number that will be used to manage the Switch via TELNET.
Syntax	**enable telnet <tcp_port_number 1-65535>**
Description	This command is used to enable the Telnet protocol on the Switch. The user can specify the TCP or UDP port number the Switch will use to listen for Telnet requests.
Parameters	*<tcp_port_number 1-65535>* – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable Telnet and configure port number:

```
DES-3800:admin#enable telnet 23
Command: enable telnet 23

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To disable the Telnet protocol on the Switch:

```
DES-3800:admin#disable telnet
Command: disable telnet

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DES-3800:admin#enable web 80
Command: enable web 80

Success.

DES-3800:admin#
```

disable web

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

Example usage:

To disable HTTP:

```
DES-3800:admin#disable web
Command: disable web

Success.

DES-3800:admin#
```

enable snmp

Purpose	Used to enable SNMP on the switch, so that it can be managed via SNMP based manafement software.
Syntax	**enable snmp**
Description	The enable snmp command enables SNMP.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable SNMP:

```
DES-3800:admin#enable snmp
Command: enable snmp

Success.

DES-3800:admin#
```

disable snmp

Purpose	Used to disable SNMP on the switch.
Syntax	**disable snmp**
Description	The disable snmp command disables SNMP.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable SNMP:

```
DES-3800:admin#disable snmp
Command: disable snmp

Success.

DES-3800:admin#
```

save

Purpose	Used to save changes in the Switch's configuration to non-volatile RAM.
Syntax	**save {config <config_id 1-2>}**
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the Switch's memory each time the Switch is restarted.
Parameters	*config <config_id 1-2>* - Choose this parameter to save the current switch configuration to a file located on the memory of the Switch. The user may enter 1 or 2 to identify this configuration file. If no *config_id* is specified, changes in the switch configuration will be saved to the current and active switch configuration file.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#save
Command: save

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

DES-3800:admin#
```

Example usage:

To save the Switch's current configuration to config_id 1 in the non-volatile RAM:

```
DES-3800:admin#save config 1
Command: save

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

DES-3800:admin#
```

reboot

Purpose	Used to restart the Switch.
Syntax	**reboot {force_agree}**
Description	The reboot command restarts the switch.
Parameters	*force_agree* - When force_agree is specified, the reboot command will be executed immediatedly without further confirmation.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To restart the Switch:

```
DES-3800:admin#reboot
Command: reboot
Are you sure to proceed with the system
reboot?(y/n)
Please wait, the switch is rebooting...
```

reset

Purpose	Used to reset all switch parameters.
Syntax	**reset {[config | system]} {force_agree}**
Description	The reset command resets all switch parameters to the factory defaults.
Parameters	*config* – If you specify the 'config' keyword , all parameters are reset to default settings. But device will not do save neither reboot. *system* – If you specify the 'system' keyword, all parameters are reset to default settings. Then the switch will do factory reset, save and reboot If no keyword is specified, all parameters will be reset to default settings except the IP address, user account and history log. But device will not save or reboot. *force_agree* - When force_agree is specified, the reset command will be executed immediatedly without further confirmation.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#reset
Command: reset


Are you sure to proceed with system reset
except IP address?(y/n)
Success.


DES-3800:admin#
```

```
DES-3800:admin#reset config
Command: reset config


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


DES-3800:admin#
```

```
DES-3800:admin#reset system
Command: reset system


Are you sure to proceed with system reset, save
and reboot?(y/n)
Loading factory default configuration... Done.
```

```
Saving all configurations to NV-RAM... Done.
Please wait, the switch is rebooting...
```

login

Purpose	Used to to initiate the login procedure 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-3800:admin#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-3800:admin#logout
```

show config

Purpose	Used to collect and show all system configurations in a single CLI command..
Syntax	**show config**
Description	This command displays all system configurations. The continuous displaying configuration can be aborted via by interrupt key, which may be a sequence of keying processes or a single key. The display format should be same as CLI configuration command.
Parameters	*current_config* *config_in_nvram <config_id 1-2>* *information*
Restrictions	None.

Example usage:

To show all system configurations from DRAM database:

```
DES-3800:admin#show config config_in_nvram
Command: show config config_in_nvram


# BASIC


config serial_port baud_rate 9600 auto_logout never
enable telnet 23
enable web 80
disable jumbo_frame


# STP


 config stp maxage 20 hellotime 2 forwarddelay 15
priority 32768 version rstp txholdcount 3 fbpdu
enabled
 disable stp
 config stp ports 1-24 cost auto priority 128 edge
false p2p auto state enabled


# LACP


config link_aggregation algorithm mac_source
config lac
```

config configuration

Purpose	Used to activate, delete or set a configuration as an active configuration.
Syntax	**config configuration**
Description	The config configuration command actives, deletes or set as boot_up configuration of the device.
Parameters	*<config_id 1-2>* *active* *delete* *boot_up*
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To activate configuration 1:

```
DES-3800:admin#config configuration 1 active
Command: config configuration 1 active

Success.

DES-3800:admin#
```

Example usage:

To delete configuration 2:

```
DES-3800:admin#config configuration 2 delete
Command: config configuration 2 delete

Success.

DES-3800:admin#
```

Example usage:

To apply configuration 1:

```
DES-3800:admin#config configuration 1 apply
Command: config configuration 1 apply

Success.

DES-3800:admin#
```

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	None.

Example usage:

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

```
DES-3800:admin#telnet 10.53.13.99 tcp_port 23
Command: telnet 10.53.13.99 tcp_port 23
```

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

Example usage:

To configure a terminal_line:

```
DES-3800:admin# config terminal_line 30
Command: config terminal_line 30

Success.

DES-3800:admin#
```

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

Example usage:

To show a terminal_line:

```
DES-3800:admin# show terminal_line
Command: show terminal_line

Current terminal line number : 30

DES-3800:admin#
```

show device_status

Purpose	Used to display the current status of the hardware of the Switch.
Syntax	**show device_status**
Description	This command displays the current status of the Switch's physical elements.
Parameters	None.
Restrictions	None.

Example usage:

To show the current hardware status of the Switch:

```
DES-3800:admin#show device_status
Command: show device_status

Internal Power    External power     Side Fan    Back Fan
--------------    --------------     --------    --------
Active            Fail               OK           None

DES-3800:admin#
```

5

SWITCH PORT COMMANDS

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

Command	Parameters
config ports	[<portlist> | all] { medium_type[fiber|copper]} { speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | description [<desc 0-32> | clear] }
show ports	{<portlist>} {[description} | err_disabled]}

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

config ports	
Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	**config ports [<portlist> | all] { medium_type[fiber|copper]} { speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | description [<desc 0-32> | clear] }**
Description	This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the *<portlist>* will be affected.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *all* – Configure all ports on the Switch. *medium_type* - Specify the medium type when the configured ports are combo ports. This is an optional parameter for configuring the medium type of the combo port. For non-combo ports the user does not need to specify the medium_type in the command *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_half*- Configures the specified range of ports to operate at 10mbps half-duplex. *10_full*- Configures the specified range of ports to operate at 10mbps full-duplex. *100_half*- Configures the specified range of ports to operate at 100mbps half-duplex. *100_full*- Configures the specified range of ports to operate at 100mbps full-duplex. *1000_full* – Gigabit ports are statically set to 1000 and cannot be set to slower speeds. *flow_control [enable* | *disable]* – Enables or disables flow control for the specified ports. *learning [enable* | *disable]* – Enables or disables the MAC address learning on the specified range of ports. *state [enable* | *disable]* – Enables or disables the specified range of ports. *description <desc 32>* - Enter an alphanumeric string of no more than 32 characters to describe a selected port interface. "clear" is a keyword in this cli command. So string "clear" is not allowed. *clear* - Enter this command to clear the port description of the selected port(s).
Restrictions	Only Administrator or Operator-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-3800:admin#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-3800:admin#
```

NOTE:Combo ports prefer to use Fiber cabling. The following are the modes that the user can use to configure the Giga port.

<*Fiber Mode*> - Auto, 1000Full

<*Copper Mode*> - Auto, 100Full/Half, 10Full/Half

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	**show ports {<portlist>} {[description} | err_disabled]}**
Description	This command is used to display the current configuration of a range of ports.
Parameters	<*portlist*> – Specifies a port or range of ports to be displayed. *description* – Adding this parameter to the show ports command indicates that a previously entered port description will be included in the display. *err_disabled* – Choosing this parameter will display ports that have been disconnected due to an error on the port, such as a Loopback Detection.
Restrictions	None.

Example usage:

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

```
DES-3800:admin#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            Link Down              Enabled
11      Enabled    Auto/Enabled            Link Down              Enabled
12      Enabled    Auto/Enabled            Link Down              Enabled
13      Enabled    Auto/Enabled            Link Down              Enabled
14      Enabled    Auto/Enabled            Link Down              Enabled
15      Enabled    Auto/Enabled            Link Down              Enabled
16      Enabled    Auto/Enabled            Link Down              Enabled
17      Enabled    Auto/Enabled            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 the switch, with their descriptions:

```
DES-3800:admin#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:
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
```

To display the Error Disabled ports:

```
DES-3800:admin#show ports err_disabled
Command : show ports err_disabled

Port         Port           Connection status      Reason
             State
----         -----          -----------------      -------
 2           Enabled        Err-disabled           Storm control
             Desc: Port 2
 8           Enabled        Err-disabled           Storm control
             Desc: Port 8
 20          Enabled        Err-disabled           Storm control
             Desc: Port 20


DES-3800:admin#
```

6

SNMP V3

The SNMP v3 commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create snmp user	<snmp_username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > | sha <auth_password 8-20 >] priv [none(1) | des <priv_password 8-16>]| by_key auth [md5 <auth_key 32-32>| sha <auth_key 40-40>] priv [none(1) | des) <priv_key 32-32>]]}
delete snmp user	<snmp_username 32>
show snmp user	
show snmp groups	
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>
create snmp host	<ipaddr> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	<ipaddr>
show snmp traps	

Each command is listed in detail in the following sections:

create snmp user

<table>
<tr><td><b>Purpose</b></td><td>Used to create a new user for an SNMP group.</td></tr>
<tr><td><b>Syntax</b></td><td><b>create snmp user <snmp_username32> <groupname32> {encrypted(1) [by_password(1) auth [md5(2) <auth_password 8-16 > | sha(3) <auth_password 8-20 >] priv [none(1) | des(2) <priv_password 8-16>] | by_key(2) auth [md5(2) <auth_key 32-32>| sha(3) <auth_key 40-40>] priv [none(1) | des(2) <priv_key 32-32>]]}</b></td></tr>
<tr><td><b>Description</b></td><td>The create snmp user command creates a new user for an SNMP group. The user can choose to input authencation and privacy by password or by key.</td></tr>
<tr><td><b>Parameters</b></td><td><i><snmp_username></i> – Specifies the name of the user on the host that connects to the agent. The range is 1 to 32.
<i><groupname></i> – Specifies the name of the group to which the user is associated. The range is 1 to 32.
<i>encrypted</i> – Specifies that the password appears in encrypted form.
<i>by_password</i> – Indicates the input password for authentication and privacy.
<i>auth md5</i> | <i>sha</i> – Indicates an authentication level setting session. The options are:
md5- The HMAC-MD5-96 authentication level.
sha- The HMAC-SHA-96 authentication level.
<i>auth_password</i>- An authentication string used by MD5 or SHA1.
<i>priv_password</i>- A privacy string used by DES.
<i>auth_key</i>- An authentication key used by MD5 or SHA1, it is a hex string type.
<i>priv_key</i>- A privacy key used by DES, it is a hex string type.</td></tr>
<tr><td><b>Restrictions</b></td><td>Only Administrator or Operator-level users can issue this command.</td></tr>
</table>

Example usage:

To create a new SNMP user called dlink:

```
DES-3800:admin#create snmp user dlink D-Link_group encrypted
by_password auth md5 1

2345678 priv des 12345678

Command: create snmp user dlink D-Link_group encrypted by_password
auth md5 1234

5678 priv des 12345678


Success.


DES-3800:admin#
```

delete snmp user

Purpose	Used to remove a user from an SNMP group and delete the associated group in SNMP
Syntax	**delete snmp user < snmp_username 32>**
Description	The delete snmp user command removes a user from a SNMP group and deletes the associated group in SNMP group..
Parameters	*<snmp_username 32>*
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete a user from an SNMP group:

```
DES-3800:admin# delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-3800:admin#
```

show snmp user

Purpose	Used to display information on every SNMP username in the group username table.
Syntax	**show snmp user**
Description	The show snmp user command displays information on every SNMP username in the group username table.
Parameters	None.
Restrictions	None.

Example usage:

To display an snmp user:

```
DES-3800:admin#show snmp user
Command: show snmp user

Username    Group Name    SNMP Version   Auth-Protocol    PrivProtocol
----------------------------------------------------------------------
initial     initial        V3            None             None
Total Entries : 1
DES-3800:admin#
```

show snmp groups

Purpose	Used to display the names of the groups on the switch, the security model, level and the status of the different views.
Syntax	**show snmp groups**
Description	The show snmp groups command displays the names of groups on the switch and the securiy model,level , the stateus of the different views.
Parameters	None.
Restrictions	None.

Example usage:

To show all snmp groups setup on the switch:

```
DES-3800:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group Name       : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv

Group Name       : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv2
Securiy Level    : NoAuthNoPriv

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

Group Name       : private
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
```

```
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv
Group Name       : private
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Securiy Model    : SNMPv2
Securiy Level    : NoAuthNoPriv

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

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

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

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

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


Group Name        : WriteGroup

ReadView Name     : CommunityView
```

create snmp view

Purpose	Used to assign views to community strings to limit which MIB objects an SNMP manager can access.
Syntax	**create snmp view <view_name 32> <oid> view_type [included | excluded]**
Description	The create snmp view assigns views to community strings to limit which MIB objects the SNMP manager can access.
Parameters	*view_name*- View name to be created. *oid*- Object- Identified tree, MIB tree *view_type*- Specifies the access type of the MIB tree in this view. The view_type options are as follows: *included*- Include this object in the view. *excluded*- Exclude this object in the view.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create a new snmp view called dlinkview:

```
DES-3800:admin# create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-3800:admin#
```

delete snmp view

Purpose	Used to remove a snmp view record.
Syntax	**delete snmp view <view_name 32> [all | <oid>]**
Description	The delete snmp view command removes a snmp view record.
Parameters	<*view_name 32*>- SNMP View name to be deleted. There are two options for deleting a view record: *all*- Specifies that all view records should be deleted. <*oid*>- Specifies that the specified Object-Identified tree, MIB tree should be deleted.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete an SNMP view:

```
DES-3800:admin# delete snmp view dlinkview all
Command: delete snmp view dlinkview all


Success.

 DES-3800:admin#
```

show snmp view

Purpose	Used to display the SNMP view records.
Syntax	**show snmp view {<view_name>}**
Description	The show snmp view command displays the SNMP view record .
Parameters	*view_name*- View name of the user who likes to show.
Restrictions	None.

Example usage:

To show the SNMP view:

```
DES-3800:admin# show snmp view
Command: show snmp view

Vacm View Table Settings

View Name : restricted
Subtree   : 1.3.6.1.2.1.1
View Type : Included
View Mask :

View Name : restricted
Subtree   : 1.3.6.1.2.1.11
View Type : Included
View Mask :

View Name : restricted
Subtree   : 1.3.6.1.6.3.10.2.1
View Type : Included
View Mask :

View Name : restricted
Subtree   : 1.3.6.1.6.3.11.2.1
View Type : Included
View Mask :

Total Entries: 4

DES-3800:admin#
```

create snmp community

Purpose	Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. You can specify one or more of the following characteristics associated with the string: An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent. A MIB view, which defines the subset of all MIB objects accessible to the given community. Read and write or read-only permission for the MIB objects accessible to the community.
Syntax	**create snmp community <community_string 32> view <view_name 32> [read_only|read_write]**
Description	The create snmp community command creates an SNMP community string.
Parameters	*community_string*- Communtiy string. Max string length is 32. *view_name*- View name. A MIB view. Max length is 32 *[read_only* | *read_write]*- Read and write or read-only permission.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create an SNMP community string:

```
DES-3800:admin#create snmp community dlink view CommunityView
read_write
Command: create snmp community dlink view CommunityView read_write

Success.

DES-3800:admin#
```

delete snmp community

Purpose	Used to remove a specific communtiy string
Syntax	**delete snmp community <community_string 32>**
Description	The delete snmp community command removes a specific community string.
Parameters	*<community_string 32>*- Type the Communtiy string that will be deleted.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete an SNMP community:

```
DES-3800:admin#delete snmp community dlink
```

```
Command: delete snmp community dlink


Success.


DES-3800:admin#
```

show snmp community

Purpose	Used to display the snmp community string configurations.
Syntax	show snmp community { <community_string> }
Description	The **show snmp communtiy** command displays the community string configurations..
Parameters	*<community_string>*- Type in the string of the community that needs to be deleted. If no specific community string is specified, all community string information will be displayed.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To display the snmp community string configurations:

```
DES-3800:admin# show snmp community
Command: show snmp community

SNMP Community Table
Community Name                   View Name                Access Right
-------------------------------  -----------------------  ------------
private                          CommunityView            read_write
Index : public
Community Name                   View Name                Access Right
-------------------------------  -----------------------  ------------
public                           CommunityView            read_only


Total Entries : 2

DES-3800:admin#
```

config snmp engineID

Purpose	Used to configure an identifier for the SNMP engine on the switch.
Syntax	**config snmp engineID**
Description	The config snmp engineID command configures a identifier for the SNMP engine on the switch. Associated with each SNMP entity is a unique engineID.
Parameters	*snmp_engineID*- Identify for the SNMP engine on the switch. It is octet string type.

config snmp engineID

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

Example usage:

To configure the SNMP engineID:

```
DES-3800:admin#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DES-3800:admin#
```

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. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent’s SNMP management private enterprise number as assigned by IANA, D_Link is 171. The fifth octet is 03 to indicates the rest is the MAC address of this device. The 6th –11th octets is MAC address.
Parameters	None.
Restrictions	None.

Example usage:

To show the snmp engine id:

```
DES-3800:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DES-3800:admin#
```

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> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]]{read_view <view_name> | notify_view <view_name> | notify_view <view_name>}**
Description	The create snmp group command creates a new SNMP group.
Parameters	*groupname*- The name of the group. *v1*- The least secure of the possible security models.

create snmp group

	v2c- The second least secure of the possible security models. *v3*- The most secure of the possible. Specifies authentication of a packet *noauth_nopriv*- Neither supports packet authentication or encryption. *auth_nopriv*- Support packet authentication . *auth_priv*- Support packet authentication and encrypting. *view_name*- The View name, a MIB view.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create an snmp group:

```
DES-3800:admin#create snmp group D-Link_group v3 auth_priv read_view
CommunityView write_view CommunityView notify_view CommunityView
Command: create snmp group D-Link_group v3 auth_priv read_view
CommunityView write_view CommunityView notify_view CommunityView

Success.

DES-3800:admin#
```

delete snmp group

Purpose	Used to remove a SNMP group.
Syntax	**delete snmp group <groupname>**
Description	The delete snmp group command removes a SNMP group.
Parameters	<groupname>-The name of the group that will be deleted.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete an snmp group:

```
DES-3800:admin#delete snmp group D_Link_group
Command: delete snmp group D_Link_group

Success.

DES-3800:admin#
```

create snmp host

Purpose	Used to create a recipient of an SNMP trap operation.
Syntax	**create snmp host <ipaddr> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>**

create snmp host

Description	The create snmp host command creates a recipient of an SNMP operation .
Parameters	ipaddr- The IP address of the recipient for which the traps are targeted. v1- The least secure of the possible security models. v2c- The second least secure of the possible security models. v3- The most secure of the possible. The v3 version has 3 additional parameters that can be specified: noauth_nopriv- Neither support packet authentication nor encrypting. Auth_nopriv- Support packet authentication . Auth_priv- Support packet authentication and encrypting. auth_string- Authentication string
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create a new SNMP host:

```
DES-3800:admin#create snmp host 10.48.74.100 v3 noauth_nopriv initial
Command: create snmp host 10.48.74.100 v3 noauth_nopriv initial

Success.

DES-3800:admin#
```

delete snmp host

Purpose	Used to delete a recipient of an SNMP trap operation.
Syntax	**delete snmp host <ipaddr>**
Description	The delete snmp host command deletes a recipient of an SNMP trap operation.
Parameters	*ipaddr-* The IP address of the recipient for which the traps are targeted.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete an SNMP host:

```
DES-3800:admin#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DES-3800:admin#
```

show snmp host

Purpose	Used to display the recipient for which the traps are targeted.
Syntax	**show snmp host {<ipaddr>}**
Description	The show snmp host command displays the recipient for which the traps are targeted.
Parameters	*{<ipaddr>}* - The IP address of the recipient for that the traps are targeted for. If no parameter specified , all snmp hosps will be diplayed.
Restrictions	None.

Example usage:

To display the SNMP hosts:

```
DES-3800:admin# show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  --------------------------------
10.48.76.100     V3 noauthnopriv  initial
10.51.17.1       V2c              public

Total Entries : 2

DES-3800:admin#
```

show snmp traps

Purpose	Used to display the status of snmp trap and authentication traps.
Syntax	**show snmp traps**
Description	The show snmp traps command is used to show the SNMP traps state.
Parameters	None.
Restrictions	None.

Example usage:

To show the SNMP trap state on the switch:

```
DES-3800:admin#show snmp traps
Command: show snmp traps

SNMP Trap           : Enabled
Authenticate Traps : Enabled

DES-3800:admin#
```

7

POE COMMANDS

DES-3828P supports Power over Ethernet (PoE) as defined by the IEEE 802.3af specification. Ports 1-24 supply 48 VDC power to PDs over Category 5 or Category 3 UTP Ethernet cables. DES-3828P follows the standard PSE pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. DES-3828P works with all D-Link 802.3af capable devices.

DES-3828P includes the following PoE features:

The auto-discovery feature recognizes the connection of a PD (Powered Device) and automatically sends power to it.

The auto-disable feature will occur under two conditions: first, if the total power consumption exceeds the system power limit; and second, if the per port power consumption exceeds the per port power limit.

The active circuit protection feature automatically disables the port if there is a short. Other ports will remain active.

PDs receive power according to the following classification:

Class	Max power used by PD
0	0.44 to 12.95W
1	0.44 to 3.84W
2	3.84 to 6.49W
3	6.49 to 12.95W

PSE provides power according to the following classification:

Class	Max power provided by PSE
0	15.4W
1	4.0W
2	7.0W
3	15.4W

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

Command	Parameters
config poe system	{power_limit <value 37-370> | power_disconnect_method [deny_next_port | deny_low_priority_port]}
config poe ports	[all | <portlist>] {state [enable | disable] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-16800>]}
show poe system	
show poe ports	{<portlist>}

Each command is listed in detail in the following sections.

config poe system

Purpose	Used to configure the parameters for the whole PoE system.
Syntax	**config poe system {power_limit <value 37-370> | power_disconnect_method [deny_next_port | deny_low_priority_port}**
Description	Allows the user to configure the parameters for the whole PoE system.
Parameters	*power_limit* - The power limit parameter allows the user to configure the power budget of whole PoE system. The minimum setting is 37 W and the maximum is 370W (depending on the power supplier's capability). Default setting is 370 W. *power_disconnect_method* -This parameter is used to configure the power management disconnection method. When the total consumed power exceeds the power budget, the PoE controller initiates a port disconnection to prevent overloading the power supply. The controller uses one of the following two ways to implement the disconnection: *deny_next_port* - After the power budget has been exceeded, the next port attempting to power up is denied, regardless of its priority. *deny_low_priority_port* - After the power budget has been exceeded, the next port attempting to power up, causes the port with the lowest priority to shut down (to allow high-priority ports to power up). The default setting is *deny_next_port*.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To config the PoE System on the Switch:

```
DES-3800:admin#config poe system power_limit 300
power_disconnect_method deny_next_port
Command: config poe system power_limit 300
power_disconnect_method deny_next_port

Success.

DES-3800:admin#
```

config poe ports

Purpose	Used to configure the PoE port settings.
Syntax	**config poe ports [all | <portlist>] {state [enable | disable] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-16800>]}**
Description	The **config poe ports** command is used to configure the PoE port settings.
Parameters	*<portlist>* -Specifies a range of ports to be configured or all the ports. *all* – Specifies that all ports (port 1-24) on the Switch will be configured for PoE. *state* - Enables or disables the PoE function on the Switch.

config poe ports	
	priority - Setting the port priority affects power-up order and shutdown order. **Power-up order**: When the Switch powers-up or reboots, the ports are powered up according to their priority (*critical* first, then *high* and finally *low*). **Shutdown order**: When the power limit has been exceeded, the ports will shut down according to their priority if the power disconnect method is set to *deny_ low_priority_port.* • *critical* – Specifying this parameter will nominate these ports has having the highest priority for all configured PoE ports. These ports will be the first ports to receive power and the last to disconnect power. • *high* – Specifying this parameter will nominate these ports as having the second highest priority for receiving power and shutting down power. • *low* – Specifying this parameter will nominate these ports as having the lowest priority for receiving and shutting down power. These ports will be the first ports to have their power disconnected if the *power_disconnect_method* chosen in the **config poe system** command is *deny_low_priority_port*. *power_limit* – Allows the user to configure the per-port power limit. If a port exceeds its power limit, the PoE system will shut down that port. The minimum user-defined setting is 1000mW and maximum is 16800mW. The default setting is 15400mW. The user may also choose to define a power class by which to set the power limit, based on the PSE table at the beginning of this section. • *class_0* – Choosing this class will set the maximum port limit at 15.4W. • *class_1* - Choosing this class will set the maximum port limit at 4.0W. • *class_2* - Choosing this class will set the maximum port limit at 7.0W. • *class_3* - Choosing this class will set the maximum port limit at 15.4.0W. • *user_define* – Choosing this parameter will allow the user to set a power limit between 1000 and 16800mW with a default value of 15400mW.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To config the Switch's ports for PoE:

```
DES-3800:admin#config poe ports 1-3 state enable priority critical
power_limit class_0
Command: config poe ports 1-3 state enable priority critical
power_limit class_0

Power limit has been set to 15400mW(Class 0 PD upper power limit
12.95W + power loss on cable).
Success.

DES-3800:admin#
```

show poe system	
Purpose	Used to display the setting and actual values of the whole PoE system.
Syntax	**show poe system {<portlist>}]**
Description	Display the settings and actual values of the whole PoE system.
Parameters	None.
Restrictions	None.

Example usage:

To display the power settings for the switch system:

```
DES-3800:admin#show poe system
Command: show poe system

PoE System Information
---------------------------------------------------
Power Limit                : 300 (watts)
Power Consumption          : 0 (watts)
Power Remained             : 300 (watts)
Power Disconnection Method : deny next port
If Power remained is less than 19 watts(Power Guard Band) and Power
Disconnection Method is set to deny next port, then no additional port
will be connected.

DES-3800:admin#
```

show poe ports	
Purpose	Used to display the settings and the actual values of the PoE ports.
Syntax	**show poe ports {<portlist>}**
Description	Display the settings, actual values and port configuration of the whole PoE system.
Parameters	*<portlist>* – Enter a port or range of ports to be display their PoE settings.
Restrictions	None.

Example usage:

To display the power settings for the switch's ports

```
DES-3800:admin#show poe ports
Command: show poe ports
Port  State     Priority   Power Limit(mW)
      Class     Power(mW)  Voltage(decivolt)  Current (mA)
      Status
=========================================================
1     Enabled   Critical   12000(User-defined)
      0         0          0                  0
      OFF   : Non-standard PD connected
2     Enabled     Critical    12000(User-defined)
      OFF   : Interim state during line detection
3     Enabled     Critical    12000(User-defined)
      OFF   : Interim state during line detection
4     Enabled     Low         15400(User-defined)
```

```
      OFF   : Interim state during line detection
5     Enabled     Low         15400(User-defined)
      OFF   : Interim state during line detection
6     Enabled     Low         15400(User-defined)
      OFF   : Interim state during line detection

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

8

NETWORK MANAGEMENT COMMANDS

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

The xStack DES-3800 Switch Series supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. After enabling SNMP, you can specify which version of SNMP you want to use to monitor and control the Switch. 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 SNMP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create trusted_host	<ipaddr> | network <ip_addr/netmask>
delete trusted_host	<ipaddr> | network <ip_addr/netmask>| all
show trusted_host	
enable snmp traps	
enable snmp authenticate traps	
show snmp traps	
disable snmp traps	
disable snmp authenticate traps	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable rmon	
disable rmon	
enable snmp	
disable snmp	

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

create trusted_host

Purpose	Used to create the trusted host.
Syntax	**create trusted_host <ipaddr> | network <ip_addr/netmask>**
Description	The **create trusted_host** command creates the trusted host. The Switch allows specification of up to three IP addresses or networks that are allowed to manage the Switch via in-band SNMP, Web or TELNET based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.
Parameters	*<ipaddr>* – The IP address of the trusted host to be created. *network<ip_addr/netmask>* – The network address of the trusted network. The form of the network address is xxx.xxx.xxx.xxx/y.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create the trusted host:

```
DES-3800:admin#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DES-3800:admin#
```

delete trusted_host

Purpose	Used to delete a trusted host entry made using the *create trusted_host* command above.
Syntax	**<ipaddr> | network <ip_addr/netmask>| all**
Description	This command is used to delete a trusted host entry made using the **create trusted_host** command above.
Parameters	*<ipaddr>* – The IP address of the trusted host. *network<ip_addr/netmask>* – The network address of the trusted network. The form of the network address is xxx.xxx.xxx.xxx/y. *all*- Specifies that all trusted host entries should be deleted.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DES-3800:admin#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DES-3800:admin#
```

show trusted_host

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

Example Usage:

To display the list of trusted hosts:

```
DES-3800:admin#show trusted_host
Command: show trusted_host

Management Stations

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

Total Entries: 1

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To enable SNMP trap support on the Switch:

```
DES-3800:admin#enable snmp traps
Command: enable snmp traps

Success.

DES-3800:admin#
```

enable snmp authenticate traps

Purpose	Used to enable SNMP authentication trap support.
Syntax	**enable snmp authenticate traps**
Description	This command is used to enable SNMP authentication trap support on the Switch.

enable snmp authenticate traps

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

Example Usage:

To turn on SNMP authentication trap support:

```
DES-3800:admin#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DES-3800:admin#
```

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	None.

Example usage:

To view the current SNMP trap support:

```
DES-3800:admin#show snmp traps
Command: show snmp traps

SNMP Traps           : Enabled
Authenticate Traps   : Enabled


DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DES-3800:admin#disable snmp traps
Command: disable snmp traps

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example Usage:

To disable the SNMP authentication trap support:

```
DES-3800:admin#disable snmp authenticate
traps
Command: disable snmp authenticate traps

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DES-3800:admin#
```

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.

config snmp system_location

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

Example usage:

To configure the Switch location for “HQ 5F”:

```
DES-3800:admin#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To configure the Switch name for “DES-3828 Switch**”:**

```
DES-3800:admin#config snmp system_name DES-3828 Switch
Command: config snmp system_name DES-3828 Switch

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To enable RMON:

```
DES-3800:admin#enable rmon
Command: enable rmon

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To disable RMON:

```
DES-3800:admin#disable rmon
Command: disable rmon

Success.

DES-3800:admin#
```

enable snmp

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

Example usage:

To enable SNMP:

```
DES-3800:admin#enable snmp
Command: enable snmp

Success.

DES-3800:admin#
```

disable snmp

Purpose	Used to disable RMON on the Switch.
Syntax	**disable snmp**
Description	This command is used, in conjunction with the **enable snmp** command above, to enable and disable SNMP on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable SNMP:

```
DES-3800:admin#disable snmp
Command: disable snmp

Success.

DES-3800:admin#
```

9

SWITCH UTILITY COMMANDS

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

Command	Parameters
download	[firmware_fromTFTP <ipaddr> <path_filename 64> {image_id <1-2>} | configuration <ipaddr> <path_filename 64> {config_id <1-2> | increment}]
config firmware image_id	<int 1-2> [delete | boot_up]
show firmware information	
show config	[current_config | config_in_nvram <config_id 1-2> | information]
config configuration	<config_id 1-2> [boot_up | active | delete]
upload	[cfg_toTFTP| log_toTFTP] <ipaddr> <path_filename 64> {config_id <1-2>}
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
traceroute	<ipaddr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value <1-9>
config pkt_to_cpu zero_ttl_ip	state
show pkt_to_cpu	

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

download	
Purpose	Used to download and install new firmware or a Switch configuration file from a TFTP server.
Syntax	**download [firmware_fromTFTP<ipaddr> <path_filename 64> {image_id <1-n>}** **| configuration <ipaddr> <path_filename 64> { config_id <1-2> | increment}]**
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	*firmware_fromTFTP-* download and install new firmware on the switch from a TFTP server. *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. The maximum length is 64. *image_id <1-n>* - Specifys the image identify number of the indicated firmware. n is the maximum support number of image which can be stroed and it's product dependent; this parameter will available while dual image is supported,if the switch does not support dual image, this parameter should not included in this command. In this product, n = 2. *config_ id <1-2>* - There are two level of download configuration *(a) Apply to system only when the config_ id is omitted.* *(b) Save to flash but not apply to system if configuration ID is*

download

	specified. *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-3800:admin#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-3800:admin#
```

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. *<int 1-2>* - Select the ID number of the firmware in the Switch's memory to be configured. *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 image 1 as a boot up section:

```
DES-3800:admin# config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DES-3800:admin#
```

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	Only Administrator-level users can issue this command.

Example usage:

To display the current firmware information on the Switch:

```
DES-3800:admin#show firmware information
Command: show firmware information

ID   Version     Size(B)    Update Time          From          User
--   --------    -------    -------------------  -----------   --------
 1   2.00-B20    1360471    00000 days 00:00:00  Serial Port   Anonymous
*2   1.00-B21    2052372    00000 days 00:00:56  10.53.13.94   admin
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-3800:admin#
```

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 <config_id 1-2> | information]

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:

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.

- *config_id 1-2* **-** Adding this parameter will allow the user to specify which configuration file out of the possible 2 files, are to be displayed.

information – Entering this parameter will display information regarding configuration files loaded and saved on the Switch.

Restrictions

None.

Example usage:

To view the current configuration settings:

```
DES-3800:admin#show config current_config
Command: show config current_config

#---------------------------------------------------------------
#                      DES-3828 Configuration
#
#                      Firmware: Build 4.50-B10
#Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.
#---------------------------------------------------------------

# DOUBLE_VLAN

Diable double_vlan

# BASIC

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

# BNR

config command_prompt default

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

Example usage:

To view saved configuration file information saved on the Switch:

```
DES-3800:admin#show config information
Command: show config information

ID  Version  Size(B) Update Time          From         User
--  -------  ------  ------------         -------      -----------
*1  4.05.B08  12961  2006/08/30 09:36:10  Local Saved
 2  (empty)

Note: * indicates the next boot up configuration
(T)  means configuration update through TELNET
(S)  means configuration update through SNMP
(W)  means configuration update through WEB

DES-3800:admin#
```

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

config configuration	
	boot up section. *active* – Entering this parameter will first load and then activate this configuration file on the switch. *delete* – Entering this parameter will delete the specified configuration section.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3800:admin# config configuration 1 boot_up
Command: config configuration 1 boot_up

Success.

DES-3800:admin#
```

upload log toTFTP	
Purpose	Used to upload the current switch settings or the switch history log to a TFTP Server.
Syntax	**upload [log_toTFTP| <ipaddr> <path_filename 64>{ config_ id <1-2>}**
Description	This command is used to upload either the Switch's current settings or the Switch's history log to a TFTP server.
Parameters	*log_toTFTP* – Specifies that the switch history log will be uploaded to the TFTP server. *<ipaddr>* – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. *<path_filename 64>* – Specifies the location of the Switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the Switch. *<configid>* - Specifies that the switch's current settings will be uploaded to the TFTP server.
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only Administrator or Operator-level users can issue this command.

Example usage:

To upload a configuration file:

```
DES-3800:admin#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-3800:admin#
```

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. Only Administrator or Operator-level users can issue this command.

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

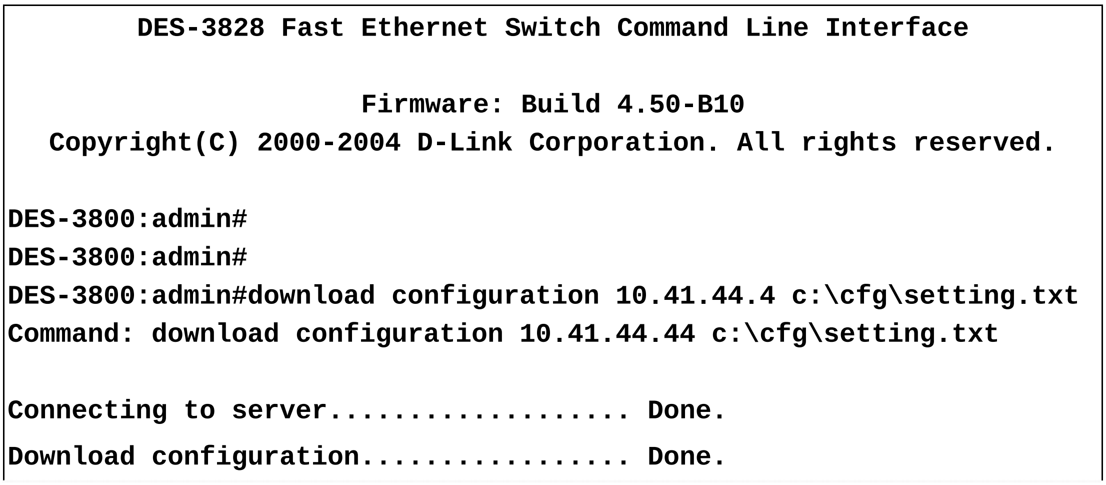
Example usage:

To enable autoconfiguration on the Switch:

```
DES-3800:admin#enable autoconfig
Command: enable autoconfig

Success.

DES-3800:admin#
```

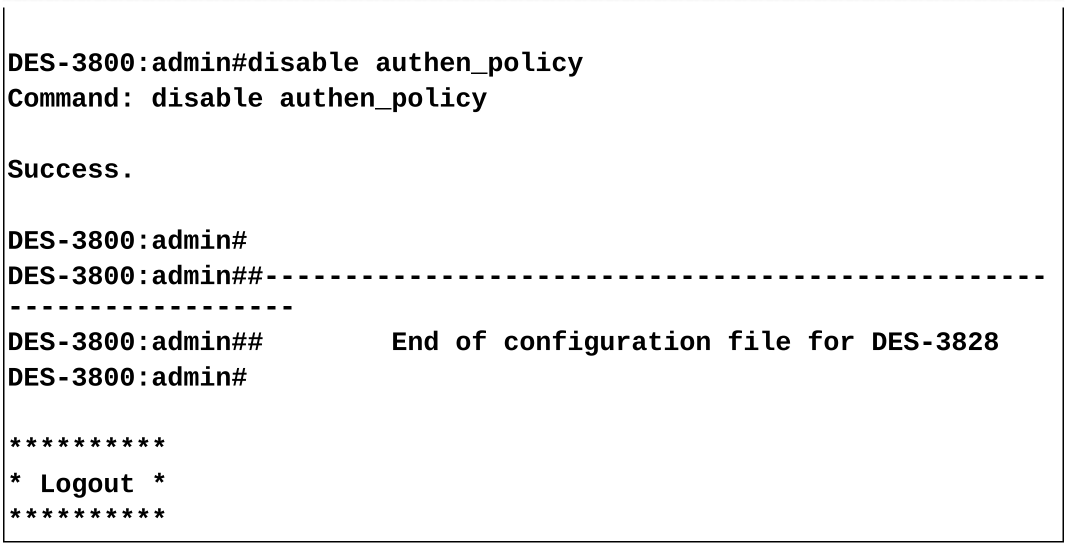
When autoconfig is enabled and the Switch is rebooted, the normal login screen will appear for a few moments while the autoconfig request (i.e. download configuration) is initiated. The console will then display the configuration parameters as they are loaded from the configuration file specified in 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-3828 Fast Ethernet Switch Command Line Interface

                          Firmware: Build 4.50-B10
   Copyright(C) 2000-2004 D-Link Corporation. All rights reserved.

DES-3800:admin#
DES-3800:admin#
DES-3800:admin#download configuration 10.41.44.4 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-3800:admin#disable authen_policy
Command: disable authen_policy

Success.

DES-3800:admin#
DES-3800:admin##----------------------------------------------------
------------------
DES-3800:admin##        End of configuration file for DES-3828
DES-3800:admin#

**********
* 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	Only Administrator or Operator-level users can issue this command.

Example usage:

To stop the autoconfiguration function:

```
DES-3800:admin#disable autoconfig
Command: disable autoconfig

Success.

DES-3800:admin#
```

show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	**show autoconfig**
Description	This will list the current status of the autoconfiguration function.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To upload an autoconfiguration-:

```
DES-3800:admin#show autoconfig
Command: show autoconfig
Autoconfig disabled.

Success.

DES-3800:admin#
```

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.

ping	
	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-3800:admin#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-3800:admin#
```

traceroute	
Purpose	Used to trace the routed path between the Switch and a destination endstation.
Syntax	**traceroute <ipaddr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value <1-9>}**
Description	The traceroute command will trace a route between the Switch and a give host on the network.
Parameters	*<ipaddr>* - Specifies the IP address of the host. *ttl <value 1-60>* - The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices. *port <value 30000-64900>* - The port number. Must be above 1024.The value range is from 30000 to 64900. *timeout <sec 1-65535>* - Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between 1 and 65535 seconds. *probe <value 1-9>* - The probe value is the number of times the Switch will send probe packets to the next hop on the intended traceroute path. The default is 1.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To trace the routed path between the Switch and 10.48.74.121.

```
DES-3800:admin#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

1  <10ms 10.254.254.251
2  <10ms 10.55.25.35
3  <10ms 10.22.35.1

DES-3800:admin#
```

config pkt_to_cpu zero_ttl_ip

Purpose	The command controls whether to capture IP packet with zero TTL to CPU.
Syntax	**config pkt_to_cpu zero_ttl_ip state [enable | disable]**
Description	The command controls whether to capture IP packets with zero TTL to CPU. In the DES-3800 series the default setting for this feature is *disable*. If you disable this feature, the device will not respond to traceroute packets.
Parameters	*state [enable* | *disable]-* Enables or disables forwarding the packet to CPU.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the forwarding packet to the CPU:

```
DES-3800:admin# config pkt_to_cpu zero_ttl_ip state enable
Command: config pkt_to_cpu zero_ttl_ip state enable

Success.
DES-3800:admin#
```

show pkt_to_cpu

Purpose	The command shows current configure that capture IP packet with zero TTL to CPU.
Syntax	show pkt_to_cpu
Description	The command displays the packet to CPU control state.
Parameters	None.
Restrictions	None.

Example usage:

To display the Zero TTL packet to CPU control state:

```
DES-3800:admin#show pkt_to_cpu
Command: show pkt_to_cpu

Zero TTL IP: Enabled
```

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 1-65535>
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 2:

```
DES-3800:admin#show packet ports 2
Command: show packet ports 2

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

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

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

show error ports

Purpose	Used to display the error statistics for a range of ports.
Syntax	**show error ports <portlist>**
Description	This command will display all of the packet error statistics collected and logged by the Switch for a given port list.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the errors of the port 3 of module 1:

```
DES-3800:admin#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

show 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-3800:admin#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          27     0         0         0
7      0        0        0          28     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
22     0        0        0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Example usage:

To display the current CPU utilization:

```
DES-3800:admin#show utilization cpu
Command: show utilization cpu

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

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To clear the counters:

```
DES-3800:admin#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To clear the log information:

```
DES-3800:admin#clear log
Command: clear log

Success.

DES-3800:admin#
```

show log

Purpose	Used to display the switch history log.
Syntax	**show log index <value 1-65535> >**
Description	This command will display the contents of the Switch's history log.
Parameters	*index <value 1-65535>* – This command will display the history log, beginning at 1 and ending at the value specified by the user in the *<value 1-65535>* field. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.

Example usage:

To display the switch history log**:**

```
DES-3800:admin#show log index 5
Command: show log index 5

Index   Time                   Log Text
-----   -------------------    ---------------------------------------
5       2008/06/19 09:36:37    Port 23 link up, 100Mbps FULL duplex
4       2008/06/19 09:36:37    Redundant Power failed
3       2008/06/19 09:36:37    Spanning Tree Protocol is disabled
2       2008/06/19 09:36:37    System cold start
1       2008/06/19 09:36:10    Configuration saved to flash (Username:
Anonymous)

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To enable the syslog function on the Switch:

```
DES-3800:admin#enable syslog
Command: enable syslog

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DES-3800:admin#disable syslog
Command: disable syslog

Success.

DES-3800:admin#
```

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-3800:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-3800:admin#
```

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, as shown below:

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

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

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

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

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

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

Numerical 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)**

create syslog host	
	17 local use 1 (local1) **18 local use 2 (local2)** **19 local use 3 (local3)** **20 local use 4 (local4)** **21 local use 5 (local5)** **22 local use 6 (local6)** **23 local use 7 (local7)** *local0* – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above. *local1* – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above. *local2* – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above. *local3* – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above. *local4* – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above. *local5* – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above. *local6* – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above. *local7* – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above. *udp_port <udp_port_number>* – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. *state [enable* | *disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create syslog host:

```
DES-3800:admin#create syslog host 1 ipaddress 10.1.1.1
state enable
Command: create syslog host 1 ipaddress 10.1.1.1 state
enable

Success.

DES-3800:admin#
```

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. *all* – Specify to configure all Syslog hosts. *severity* – Severity level indicator. These are described in the following: Bold font indicates that the corresponding severity level is currently supported on the Switch.

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

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

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

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

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

config syslog host

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.

ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent.

state [enable **|** *disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.

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

Example usage:

To configure a syslog host:

```
DES-3800:admin#config syslog host 1 severity all
facility local0
Command: config syslog host all severity all facility
local0

Success.

DES-3800:admin#
```

Example usage:

To configure a syslog host for all hosts:

```
DES-3800:admin#config syslog host all severity all
facility local0
Command: config syslog host all severity all facility
local0

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DES-3800:admin#delete syslog host 4
Command: delete syslog host 4

Success.

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

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.

config system_severity

	- *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 or Operator-level users can issue this command.

Example usage:

To configure the system severity settings for critical traps only:

```
DES-3800:admin#config system_severity trap critical
Command: config system_severity trap critical

Success.

DES-3800:admin#
```

show system_severity

Purpose	To display the current severity settings set on the Switch.
Syntax	**show system_severity**
Description	This command is used to view the severity settings that have been implemented on the Switch using the **config system_severity** command.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To view the system severity settings currently implemented on the Switch:

```
DES-3800:admin#show system_severity
Command: show system_severity

system_severity log     :   information
system_severity trap    :   critical

DES-3800:admin#
```

11

LAYER 2 FDB 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>
config multicast port_filtering_mode	[<portlist> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]
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}
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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#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-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To create multicast MAC forwarding**:**

```
DES-3800:admin#create multicast_fdb default 01-00-
00-00-00-01
Command: create multicast_fdb default 01-00-00-00-
00-01

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DES-3800:admin#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-3800:admin#
```

NOTE: When IGMP Snooping is enabled, the Static Multicast Forwarding settings will not take effect.

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 or Operator-level users can issue this command.

Example usage:

To set the FDB aging time:

```
DES-3800:admin#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3800:admin#
```

config multicast port_flitering_mode

Purpose	Used to configure the multicast packet filtering mode for ports.
Syntax	**config multicast port_filtering_mode [<portlist>|all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]**
Description	The config multicast port_filtering_mode command configures the multicast packet filtering mode for all ports.
Parameters	*<portlist>* – Specifies a range of ports to be configured. *all* – Specifies that all ports will be configured. *forward_all_groups-* In this mode frames destined for group MAC addresses are forwarded according to the VLAN rule. *forward_unregistered_groups-* In this mode, if the Group MAC Address Registration entries exist in the Multicast Table, frames destined for the corresponding Group MAC addresseses are forwarded, only on ports identified in the member port set. If the Group MAC address does not exist in the Multicast Table the frames are forwarded according to the VLAN rule. *filter_unregistered_groups-* In this mode frames destined for group MAC addresses are forwarded only if this type of forwarding is explicitly permitted by a Group Address entry in the Multicast Table. In other words, if the Group MAC address does not exist in the Multicast table, the packets are dropped.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the multicast packet filtering mode for ports:

```
DES-3800:admin#config multicast
port_filtering_mode 15:1-15:4 forward_all_groups
Command: config multicast port_filtering_mode
15:1-15:4 forward_all_groups


Success.


DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DES-3800:admin# delete fdb default 00-00-00-00-
01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries**:**

```
DES-3800:admin#clear fdb all
Command: clear fdb all

Success.

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

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-3800:admin#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300
```

```
VID   VLAN Name      MAC Address            Port        Type
---   ---------      -----------            ----        --------
1     default        00-00-39-34-66-9A      10          Dynamic
1     default        00-00-51-43-70-00      10          Dynamic
1     default        00-00-5E-00-01-01      10          Dynamic
1     default        00-00-74-60-72-2D      10          Dynamic
1     default        00-00-81-05-00-80      10          Dynamic
1     default        00-00-81-05-02-00      10          Dynamic
1     default        00-00-81-48-70-01      10          Dynamic
1     default        00-00-E2-4F-57-03      10          Dynamic
1     default        00-00-E2-61-53-18      10          Dynamic
1     default        00-00-E2-6B-BC-F6      10          Dynamic
1     default        00-00-E2-7F-6B-53      10          Dynamic
1     default        00-00-E2-82-7D-90      10          Dynamic
1     default        00-00-F8-7C-1C-29      10          Dynamic
1     default        00-01-02-03-04-05      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
```

show multicast port_filtering_mode

Purpose	Used to show the multicast packet filtering mode for ports.
Syntax	**show multicast port_filtering_mode {<portlist>}**
Description	The show multicast port_filtering_mode command show the multicast packet filtering mode for ports..
Parameters	<*portlist*>- Specifies a range of ports to be configured. (UnitID:port number). If no parameter specified , the deivce will show all multicast filtering settings in the device.
Restrictions	None.

Example usage:

To show the multicast port filtering mode**:**

```
DES-3800:admin#show multicast port_filtering_mode
Command: show multicast port_filtering_mode

Port    Multicase Filter Mode
------    ---------------------------
1         forward_all_groups
2         forward_all_groups
3         forward_all_groups
4         forward_all_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        filter_unregistered_groups
12        filter_unregistered_groups

DES-3800:admin#
```

12

PACKET STORM CONTROL COMMANDS

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase 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	[<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | Unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | time_interval <sec 5-30> | countdown [0 | <minute 5-30>]}
show traffic control	{[all | <portlist>]}
config traffic control_trap	[none | storm_occurred | storm_cleared | both]

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

config traffic control

Purpose	Used to configure broadcast/multicast/Unicast packet storm control. The software mechanism is provided to monitor the traffic rate in addition to the hardware storm control mechanism previously provided.
Syntax	**config traffic control [<portlist> | all] { broadcast [enable| disable]| multicast [enable| disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value>|time_interval <secs 5-30 > | countdown <minutes 0 | 5-30>}**
Description	This command is used to configure broadcast/multicast/Unicast storm control. By adding the new software traffic control mechanism, the user can now use both a hardware and software mechanism, the latter of which will now provide shutdown, recovery and trap notification functions for the Switch.
Parameters	*<portlist>* – Used to specify a range of ports to be configured for traffic control. *all* – Specifies all ports are to be configured for traffic control on the Switch. *broadcast [enable | disable]* – Enables or disables broadcast storm control. *multicast [enable | disable]* – Enables or disables multicast storm control. *Unicast [enable | disable]* – Enables or disables traffic control.

config traffic control	
	Unicast - Enable or disable unknow packet strom control . (Only support HW storm 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/Unicast packets, in packets per second (pps), 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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin# 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

Success.

DES-3800:admin#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	**show traffic control {[all | <portlist>]}**
Description	This command displays the current storm traffic control configuration on the Switch.
Parameters	*all* - Used to specify all ports for which to display traffic control settings. *<portlist>* - Used to specify port or list of ports for which to display traffic control settings. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display traffic control setting for ports 1-4:

```
DES-3800:admin#show traffic control 1-4
Command: show traffic control 1-4

Traffic Storm Control Trap: [Occurred]

Port  Broadcast/     Multicast /    Unicast /      Action   Time       Count
      Threshold      Threshold      Threshold               Interval   down
----- -------------- -------------- -------------- -------- ---------- ------
1     Disabled/128000 Disabled/128000 Disabled/128000 drop     5          0
2     Disabled/128000 Disabled/128000 Disabled/128000 drop     5          0
3     Disabled/128000 Disabled/128000 Disabled/128000 drop     5          0
4     Disabled/128000 Disabled/128000 Disabled/128000 drop     5          0

Total Entries: 5

DES-3800:admin#
```

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 or Operator-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-3800:admin# config traffic control_trap both
Command: config traffic control_trap both

Success.

DES-3800:admin#
```

13

QOS COMMANDS

The xStack DES-3800 Series supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 7 (Class 7) — 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 Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the eight hardware priority queues in order, beginning with the highest priority queue, 7, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

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

Command	Parameters
config bandwidth_control	<portlist>{rx_rate [no_limit | <value 64-1000000>] | tx_rate [no_limit | <value 64-1000000>]}
show bandwidth_control	{<portlist>}
config scheduling	<class_id 0-n> max_packet <value 0-255>
config scheduling_mechanism	[strict(1) | weight_robin (2)]
show scheduling	
show scheduling_mechanism	
config 802.1p user_priority	<priority 0-7> <class_id 0-7>
show 802.p 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 the port bandwidth control.
Syntax	**config bandwidth_control <portlist>{rx_rate [no_limit | <value 64-1000000>] | tx_rate [no_limit | <value 64-1000000>]}**
Description	The config bandwidth_control command configures the port bandwidth control.
Parameters	*<portlist>*- Specifes a range of ports to be configured. *rx_rate*- Specifies the limitation of receive data rate. *no_limit* indicates no limitation , a value from 64 to 1000000 indicates the limitation in kbits/sec . The switch will choose the closest value and NOT a greater value in order to work. *tx_rate*- Specifies the limitation of transmit data rate. *no_limit* indicates no limitation , a value from 64 to 1000000 indicates the limitation in kbits/sec . The switch will choose the closest value, but it must NOT be greater than the value in order to work .
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the port bandwidth:

```
DES-3800:admin#config bandwidth_control 1-10 tx_rate
640
Command: config bandwidth_control 1-10 tx_rate 640

Success.

DES-3800:admin#
```

show bandwidth_control

Purpose	Used to display the port bandwidth control table.
Syntax	**show bandwidth_control {<portlist>}**
Description	The show bandwidth_control command displays the port bandwidth configurations.
Parameters	*<portlist>*- Specifies a range of ports to be displayed. If no parameter specified , system will display all the ports bandwidth configurations
Restrictions	None.

Example usage:

To display the port bandwidth control table for ports 1 to 10:

```
DES-3800:admin#show bandwidth_control  1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

Port    RX Rate       TX Rate       Effective RX        Effective TX
        (kbit/sec)    (kbit/sec)    (kbit/sec)          (kbit/sec)
```

```
------  ----------    ----------    ---------------     --------------
1       no_limit      no_limit      no_limit            no_limit
2       no_limit      no_limit      no_limit            no_limit
3       no_limit      no_limit      no_limit            no_limit
4       no_limit      no_limit      no_limit            no_limit
5       no_limit      no_limit      no_limit            no_limit
5       no_limit      no_limit      no_limit            no_limit
7       no_limit      no_limit      no_limit            no_limit
8       no_limit      no_limit      no_limit            no_limit
9       no_limit      no_limit      no_limit            no_limit
10      no_limit      no_limit      no_limit            no_limit

DES-3800:admin#
```

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling <class_id 0-n> max_packet <value 0-15>**
Description	The switch contains n+1 hardware priority queues. Incoming packets must be mapped to one of these n+1 queues. This command is used to specify the rotation by which these n+1 hardware priority queues are emptied. In this product, n = 7. The max_packets parameter allows you 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 15 can be specified. For example, if a value of 3 is specified, then the highest hardware priority queue (number n) will be allowed to transmit 3 packets – then the next lowest hardware priority queue (number n-1) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat.
Parameters	*class_id*- This specifies which of the n+1 hardware priority queues the config scheduling command will apply to. The four hardware priority queues are identified by number from 0 to ñ with the 0 queue being the lowest priority. *max_packet*- Specifies the maximium 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 15 can be specified.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure traffic scheduling:

```
DES-3800:admin# config scheduling 0 max_packet 12
Command: config scheduling 0 max_packet 12

Success.

DES-3800:admin#
```

config scheduling_mechanism

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling_mechanism [strict(1) | weight_robin (2)]**
Description	This command is used to specify how the switch handle packets in priority queues.
Parameters	*strict*-The highest queue will be processed first.That is,the highest queue should finish first. *weight_robin*- Use the weighted round robin algorithm to handle packets in priority queues.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DES-3800:admin#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DES-3800:admin#
```

show scheduling

Purpose	Used to display the current traffic scheduling parameters in use on the switch.
Syntax	**show scheduling**
Description	The show scheduling command displays the current traffic scheduling parameters that are in use on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the traffic scheduling parameters for each COS queue:

```
DES-3800:admin# show scheduling
Command: show scheduling

QOS Output Scheduling

Class ID  MAX. Packets
--------  ------------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8
```

```
DES-3800:admin#
```

show scheduling_mechanism

Purpose	Used to show the traffic scheduling mechanism.
Syntax	**show scheduling_mechanism**
Description	The show scheduling_mechanism command displays the traffic scheduling mechanism.
Parameters	None.
Restrictions	None.

Example usage:

To show scheduling_mechanism:

```
DES-3800:admin# show scheduling_mechanism
Command: show scheduling_mechanism

Success.

DES-3800:admin#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the switch.
Syntax	**config 802.1p user_priority <priority 0-7> <class_id 0-n>**
Description	The config 802.1p user_priority command allows you to configure the way the switch will map an incoming packet, based on its 802.1p user priority, to one of the eight available hardware priority queues on the switch. The switch's default setting is to map the incoming 802.1p user priority values to the eight hardware priority queues:. This product supports 8 CoS queues. You can change this mapping by specifying the 802.1p user priority you want by specifying the number of the hardware queue in the <class_id> parameter.
Parameters	*<priority 0-7>*- The 802.1p user priority you want to associate with the <class_id 0-n> (the number of the hardware queue) with. *<class_id 0-n>*- The number of the switch's hardware priority queue. The switch has n+1 hardware priority queues available. They are numbered between 0 (the lowest priority) and n (the highest priority).
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the 802.1p user priority:

```
DES-3800:admin# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-3800:admin#
```

show 802.1p user_priority

Purpose	Used to display 802.1p user priority
Syntax	**show 802.1p user_priority**
Description	The show 802.1p user_priority command displays the 802.1p user priority.
Parameters	None.
Restrictions	None.

Example usage:

To display the traffic scheduling mechanism for each COS queue:

```
DES-3800:admin# show 802.1p user_priority
Command: show 802.1p user_priority

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

DES-3800:admin#
```

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	The config 802.1p default_priority command allows you to specify default priority handling of untagged packets received by the switch. The priority value entered with this command will be used to determine which of the four hardware priority queues the packet will be forwarded to.
Parameters	*portlist*- This specifies a range of ports for which the default priority is to be configured. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separeted by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, 3 would specify switch port 3. 4 specifies switch port 4. 3-4 specifies all of the ports between switch port 3 and port 4 − in numerical order. *all*- Specifies that the command applies to all ports on the switch. *priority*- The priority value (0 to 7)you want to assign to untagged packets received by the switch or a range of ports on the switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the 802.1p default priority settings on the switch::

```
DES-3800:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3800:admin#
```

show 802.1p default_priority

Purpose	Used to display the current default priority settings on the switch.
Syntax	**show 802.1p default_priority { <portlist> }**
Description	The show 802.1p default_priority command displays the current default priority settings on the switch.
Parameters	*<portlist>*- Specified a range of ports to be displayed. If no parameter specified , the system will display all ports configured with 802.1p default_priority.
Restrictions	None.

Example usage:

To display 802.1p default priority:

```
DES-3800:admin# show 802.1p default_priority
Command: show 802.1p default_priority

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

```
21               0            0
22               0            0
23               0            0
24               0            0
25               0            0
26               0            0
27               0            0
28               0            0
DES-3800:admin#
```

14

MIRROR CONFIGURATION 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, you can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	*<port>* – This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be 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]* – Specify 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	Only Administrator or Operator-level users can issue this command.The Target port cannot be listed as a source port.

Example usage:

To add the mirroring ports:

```
DES-3800:admin# config mirror port 1 add source ports
2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

DES-3800:admin#
```

Example usage:

To delete the mirroring ports:

```
DES-3800:admin#config mirror port 1 delete source port
2-4
Command: config mirror 1 delete source 2-4

Success.

DES-3800:admin#
```

enable mirror

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

Example usage:

To enable mirroring configurations:

```
DES-3800:admin#enable mirror
Command: enable mirror

Success.

DES-3800:admin#
```

disable mirror

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

Example usage:

To disable mirroring configurations:

```
DES-3800:admin#disable mirror
Command: disable mirror

Success.

DES-3800:admin#
```

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-3800:admin#show mirror
Command: show mirror

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

DES-3800:admin#
```

15

VLAN COMMANDS

Along with normal VLAN configurations, this Switch now incorporate Double VLANs. Better known as Q-IN-Q VLANs, Double VLANs allow network providers to expand their VLAN configurations to place VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over complicating configurations on the client's side. Not only will over-complication be avoided, but now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network.

Implementation of this feature adds a VLAN frame to an existing VLAN frame for the ISP VLAN recognition and classification. To ensure devices notice this added VLAN frame, an Ethernet encapsulation, here known as a tpid, is also added to the frame. The device recognizes this tpid and therefore checks the VLAN tagged packet to see if a provider VLAN tag has been added. If so, the packet is then routed through this provider VLAN, which contains smaller VLANs with similar configurations to ensure speedy and guaranteed routing destination of the packet.

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}
show vlan	{<vlan_name 32>}
config vlan	<vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}
delete vlan	<vlan_name 32>
create vlan vlanid	<vidlist> {advertisement}
show vlan vlanid	<vidlist>
config vlan vlanid	<vidlist> {add [tagged | untagged | forbidden] | delete <portlist> | advertisement [enable | disable] | name <name>}
delete vlan vlanid	<vidlist>
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 gvrp	{<portlist>}
create dot1v_protocol_group group_id	<id>
config dot1v_protocol_group group_id	< id> [add | delete] protocol [ethernet_2| ieee802.3_snap| ieee802.3_llc] < protocol_value>
delete dot1v_protocol_group	[group_id <id> | all]
show dot1v_protocol_group	{group_id <id>}
config port dot1v ports	<portlist> | all] [add protocol_group group_id <id> vlan< vlan_name 32> | delete protocol_group [group_id <id>|all]
show port dot1v	{ports <portlist>}
enable pvid auto_assign	
disable pvid auto_assign	

Command	Parameters
show pvid auto_assign	

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 creation of 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	Only Administrator or Operator-level users can issue this command.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 4k static VLANs may be created per configuration.

Example usage:

To create a VLAN v1, tag 2:

```
DES-3800:admin#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

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 is used to add ports to the port list of a previously configured VLAN. The additional ports can be specified 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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DES-3800:admin#
```

To delete ports from a VLAN:

```
DES-3800:admin#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.
```

```
DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To remove the VLAN “v1”:

```
DES-3800:admin#delete vlan v1
Command: delete vlan v1

Success.

DES-3800:admin#
```

create vlan vlanid

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

Example usage:

To create a VLAN with VLAN ID 2 and VLAN ID 3:

```
DES-3800:admin#create vlan vlanid 2-3
Command: create vlan vlanid 2-3

Success.

DES-3800:admin#
```

show vlan vlanid

Purpose	Used to display a previously configured VLAN by VLAN ID on the Switch.
Syntax	**show vlan vlanid <vidlist>**
Description	The show VLAN by vlanid command is used to display a previously configured VLAN on the Switch.
Parameters	*<vidlist>* - Specifies the VID range from the configured VLANs set on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To display a previously created VLAN:

```
DES-3800:admin#show vlan vlanid 99
Command: show vlan vlanid 99

VID               : 99         VLAN Name     : robert
VLAN TYPE         : static     Advertisement : Enabled
Member ports      : 1-4
Static ports      : 1-4
Current Tagged ports    : 1-4
Current Untagged ports  :
Static Tagged ports     : 1-4
Static Untagged ports   :
Forbidden ports :

Total Entries : 1

DES-3800:admin#
```

config vlan vlanid

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan vlanid <vidlist> {add [tagged | untagged | forbidden] | delete <portlist> | advertisement [enable | disable] | name <name>}**
Description	The config vlan vlanid command allows you to add or delete ports of the port list of previously configured VLAN(s). You can specify the additional ports as being tagged, untagged or forbidden.The same port is allowed to be an untagged member port of multiple VLAN's. You can also specify if the ports will join GVRP or not with the *advertisement* parameter. The *name* parameter allows you to specify the name of the VLAN that needs to be modified.
Parameters	*<vidlist>* – Specifies a range of VLAN ID's to add ports to. *add* – Entering the add parameter will add ports to the VLAN. There are three types of ports to add: • *tagged* – Specifies the additional ports as tagged. • *untagged* – Specifies the additional ports as untagged. • *forbidden* – Specifies the additional ports as forbidden *delete*- Entering the delete the ports from the VLAN. *<portlist>* – A port or range of ports to add to the VLAN. *advertisement*- Entering the advertisement parameter specifies if the

config vlan vlanid

	port should join GVRP or not. There are two parameters: ▪ *enable*- Specifies that the port should join GVRP. ▪ *disable*- Specifies that the port should not join GVRP. *name*- Entering the name parameter specifies the name of the VLAN to be modified. ▪ <*name*>- Enter a name for the VLAN
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To add ports 4 through to 8 as tagged ports to VLAN ID 2 and VLAN ID 3:

```
DES-3800:admin#config vlan vlanid 2-3 add tagged 4-8
Command: config vlan vlanid 2-3 add tagged 4-8

Success.

DES-3800:admin#
```

Example usage:

To enable the VLAN ID 2 and VLAN ID 3 advertisment:

```
DES-3800:admin#config vlan vlanid 2-3 advertisement
enable
Command: config vlan vlanid 2-3 advertisement enable

Success.

DES-3800:admin#
```

Example usage:

To modify the name of VLAN ID 2:

```
DES-3800:admin#config vlan vlanid 2 name vlan_2
Command: config vlan vlanid 2 name vlan_2

Success.

DES-3800:admin#
```

delete vlan vlanid

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

Example usage:

To remove VLAN ID 2 and VLAN ID 3:

```
DES-3800:admin#delete vlan vlanid 2-3
Command: delete vlan vlanid 2-3

Success.

DES-3800:admin#
```

config gvrp

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

Example usage:

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

```
DES-3800:admin#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-3800:admin#
```

NOTE: The Switch supports up to 4k Dynamic Entries.

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 or Operator-level users can issue this command.

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DES-3800:admin#enable gvrp
Command: enable gvrp

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DES-3800:admin#disable gvrp
Command: disable gvrp

Success.

DES-3800:admin#
```

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-3800:admin#show gvrp
Command: show gvrp

Global GVRP : Disabled

Port  PVID  GVRP      Ingress Checking  Acceptable Frame Type
----  ----  --------  ----------------  ----------------------
1     1     Disabled  Enabled           All Frames
2     1     Disabled  Enabled           All Frames
3     1     Disabled  Enabled           All Frames
4     1     Disabled  Enabled           All Frames
5     1     Disabled  Enabled           All Frames
6     1     Disabled  Enabled           All Frames
7     1     Disabled  Enabled           All Frames
8     1     Disabled  Enabled           All Frames
9     1     Disabled  Enabled           All Frames
10    1     Disabled  Enabled           All Frames
11    1     Disabled  Enabled           All Frames
12    1     Disabled  Enabled           All Frames
13    1     Disabled  Enabled           All Frames
14    1     Disabled  Enabled           All Frames
15    1     Disabled  Enabled           All Frames
16    1     Disabled  Enabled           All Frames
17    1     Disabled  Enabled           All Frames
18    1     Disabled  Enabled           All Frames
19    1     Disabled  Enabled           All Frames
20    1     Disabled  Enabled           All Frames
21    1     Disabled  Enabled           All Frames
22    1     Disabled  Enabled           All Frames
23    1     Disabled  Enabled           All Frames
24    1     Disabled  Enabled           All Frames
25    1     Disabled  Enabled           All Frames
26    1     Disabled  Enabled           All Frames
27    1     Disabled  Enabled           All Frames
28    1     Disabled  Enabled           All Frames

Total Entries : 28

DES-3800:admin#
```

create dot1v_protocol_group group_id

Purpose	Create a protocol group for the protocol VLAN function.
Syntax	**create dot1v_protocol_group group_id < id>**
Description	create a protocol group for protocol VLAN function
Parameters	<*id*> - The id number of the protocol group which is used to identify a set of protocols
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create a protocol group

```
DES-3800:admin#create dot1v_protocol_group group_id 100
Command: create dot1v_protocol_group group_id 100

Success.
DES-3800:admin#
```

config dot1v_protocol_group group_id

Purpose	Configure a previously created protocol group.
Syntax	**config dot1v_protocol_group group_id <id>** **[add | delete] protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] < protocol_value>**
Description	This command configures a previously created protocol group.
Parameters	*group_id* - The id of the protocol group which needs configuring. *add* | *delete* – Adds or Deletes a protocol to the protocol group. *protocol*- The protocol that will be used for the dot1v protocol group. *<protocol_value>* - The protocol value is used to identify a protocol of the frame type specified. Depending on the frame type, the octet string will have one of the following values: The form of the input is 0x0 to 0xffff. For 'ethernet'II, this is a 16-bit (2-octet) hex value. Example: Ipv4 is 800, ipv6 is 86dd, ARP is 806,.. and so on. For ' IEEE802.3 SNAP ', this is this is a 16-bit (2-octet) hex value. Example: Ipv4 is 800, ipv6 is 86dd, ARP is 806,.. and so on. For 'IEEE802.3 LLC', this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair: first octet for Destination Service Access Point (DSAP) and second octet for Source.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To add a protocol ipv6 to protocol group 100.

```
DES-3800:admin# config dot1v_protocol_group group_id
100 add protocol  ethernet_2  0x86dd
Command: config dot1v_protocol_group group_id 100 add
protocol  ethernet_2  0x86dd


Success.
DES-3800:admin#
```

delete dot1v_protocol_group group_id

Purpose	Delete a protocol group.
Syntax	**delete dot1v_protocol_group [group_id <id> | all]**
Description	This command deletes a protocol group.
Parameters	*group_id* - Specifies the group ID to be deleted. *all* - All groups.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete protocol group 100.

```
DES-3800:admin#delete dot1v_protocol_group group_id 100
Command: delete dot1v_protocol_group group_id 100

Success.
DES-3800:admin#
```

show dot1v_protocol_group

Purpose	Display the protocols defined in a protocol group.
Syntax	**show dot1v_protocol_group {group_id <id>}**
Description	Display the protocols defined in protocol groups.
Parameters	group_id - Specifies the ID of the group to be displayed if group id is not specified, all configured protocol groups will be displayed.
Restrictions	None.

Example usage:

To display the protocol group ID 100.

```
DES-3800:admin# show dot1v_protocol_group group_id 100
Command: show dot1v_protocol_group group_id 100

Protocol Group ID   Frame Type     Protocol Value
-----------------   ----------     --------------
100                 EthernetII     0x86DD

DES-3800:admin#
```

config port dot1v ports

Purpose	Assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured
Syntax	**config port dot1v ports <portlist> | all [add protocol_group group_id <id> vlan< vlan_name 32> | delete protocol_group [group_id <id>|all]**
Description	Assigns the VLAN for untagged packets ingress from the portlist based on the protocol group configured. This assignment can be removed by using delete protocol_group option
Parameters	<*portlist*> - Specifies a range of ports to apply this command. <*id*> - Group ID of the protocol group. <*vlan_name 32*> - Vlan that is to be associated with this protocol group on this port
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

The example is to assign VLAN marketing-1 for untaged ipv6 packet ingress from port 3. To configure the group ID 100 on port 3 to be associated with VLAN marketing-1.

```
DES-3800:admin#config port dot1v ports 3 add
protocol_group group_id 100 vlan marketing-1
Command: config port dot1v ports 3 add protocol_group
group_id 100 vlan marketing-1

Success.
DES-3800:admin#
```

show port dot1v

Purpose	Display the VLAN to be associated with untagged packet ingressed from a port based on the protocol group.
Syntax	**show port dot1v {ports <portlist>}**
Description	Display the VLAN to be associated with untagged packet ingressed from a port based on the protocol group.
Parameters	*portlist* - Specifies a range of ports to be displayed. If not specified, information for all ports will be displayed
Restrictions	None.

Example usage:

The example display the protocol VLAN information for ports 1 – 2.

```
DES-3800:admin# show port dot1v ports 1-2
Command: show port dot1v ports 1-2

Port : 1
Protocol Group ID     VLAN Name
-----------------  -----------------------------
1                     default
2                     vlan_2
3                     vlan_3
4                     vlan_4

Port : 2
Protocol Group ID     VLAN Name
-----------------  -----------------------------
1                     vlan_2
2                     vlan_3
3                     vlan_4
4                     vlan_5

DES-3800:admin#
```

enable pvid auto_assign

Purpose	Used to enable auto assignment of pvid
Syntax	**enable pvid auto_assign**
Description	The command enables the auto-assign of PVID. If "Auto-assign PVID" is enabled, the PVID will possibly be changed by the PVID or VLAN configuration. When a user configures a port to VLAN X's be untagged membership, this port's PVID will be updated with VLAN X. In the form of VLAN list command, PVID is updated with last item of VLAN list. When a user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned with "default VLAN".
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the enable the auto assignment of pvid:

```
DES-3800:admin#enable pvid auto_assign

Command: enable pvid auto_assign

Success.

DES-3800:admin#
```

disable pvid auto_assign

Purpose	Used to disable auto assignment of pvid
Syntax	**disable pvid auto_assign**
Description	This command disables auto-assign of pvid. If "auto-assign PVID" is disabled, PVID only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the enable the auto assignment of pvid:

```
DES-3800:admin#disable pvid auto_assign

Command: disable pvid auto_assign

Success.

DES-3800:admin#
```

show pvid auto_assign

Purpose	Used to display the PVID auto-assignment state.
Syntax	**show pvid auto_assign**
Description	This command is used to display the PVID auto-assignment state.
Parameters	None.
Restrictions	None.

```
DES-3800:admin#show pvid auto_assign
Command: show pvid auto_assign

Auto assign pvid : enabled

DES-3800:admin#
```

16

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 1-32> {type [lacp | static]}
delete link_aggregation group_id	<value 1-32>
config link_aggregation group_id	<value1-32> {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 1-32> | algorithm}

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 1-32> {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 32 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 or Operator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DES-3800:admin#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DES-3800:admin#
```

delete link_aggregation group_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value 1-32>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	*<value 1-32>* – 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 or Operator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DES-3800:admin#delete link_aggregation
group_id 6
Command: delete link_aggregation group_id 6

Success.

DES-3800:admin#
```

config link_aggregation group_id

Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-32> {master_port <port> | ports <portlist> | state [enable | disable]**
Description	This command allows you to configure a link aggregation group that was created with the **create link_aggregation** command above. The DES-3800 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 32>* – Specifies the group ID. The Switch allows up to 32 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 or Operator-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-3800:admin#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-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3800:admin#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the Switch.
Syntax	**show link_aggregation {group_id <value 1-32> | algorithm}**
Description	This command will display the current link aggregation configuration of the Switch.
Parameters	*<value 1-32>* – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups. *algorithm* – Allows you to specify the display of link aggregation by the algorithm in use by that group.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DES-3800:admin#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-3800:admin#
```

17

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] | fast_leave [enable | disable]}
config igmp_snooping querier	[<vlan_name 32> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable]}
config router_ports	<vlan_name 32> [add | delete] <portlist>
enable igmp_snooping	{forward_mcrouter_only}
show igmp_snooping	{vlan <vlan_name 32>}
disable igmp_snooping	{forward_mcrouter_only}
show igmp snooping group	vlan <vlan_name 32>
show router_ports	{vlan <vlan_name 32>} {static | dynamic}
show igmp_snooping forwarding	{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]} | fast_leave [enable | disable]}**
Description	This command allows users 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. *fast_leave [enable | disable]* – This parameter allows the user to enable the *fast leave* function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-3800:admin#config igmp_snooping default host_timeout 250
state enable
Command: config igmp_snooping default host_timeout 250 state
enable

Success.

DES-3800:admin#
```

NOTE: The *Fast Leave* function in the **config igmp_snooping** command can only be implemented if IGMP is disabled for all IP interfaces on the Switch. Configuring this function when IGMP is enabled will produce the error message “*Cannot set Fast leave when IGMP is running*” and consequently will not be implemented.

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. You might want to increase this value if you expect a subnet to be lossy.

config igmp_snooping querier

	Although 1 is specified as a valid entry, the roubustness variable should not be one or problems may arise. *last_member_query_interval <sec 1-25>* – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You may lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. *state [enable | disable]* – Allows the Switch to be specified as an IGMP Querier or Non-querier.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-3800:admin#config igmp_snooping querier default query_interval
125 state enable
Command: config igmp_snooping querier default query_interval 125
state enable

Success.

DES-3800:admin#
```

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 designation of 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	*add | delete* – Specify whether to add or delete ports as router ports. *<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 or Operator-level users can issue this command.

Example usage:

To set up static router ports:

```
DES-3800:admin#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DES-3800:admin#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**enable igmp_snooping {forward_mcrouter_only}**
Description	This command allows enabling of 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 or Operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DES-3800:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-3800:admin#
```

disable igmp_snooping

Purpose	Used to disable 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 or Operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DES-3800:admin#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-3800:admin#
```

Example usage:

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

```
DES-3800:admin#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only

Success.

DES-3800:admin#
```

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-3800:admin#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
 Fast Leave                 : Enabled

 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
 Fast Leave                 : Enabled

Total Entries: 2

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

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-3800:admin#show router_ports
Command: show router_ports

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

Total Entries: 1

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

18

802.1X COMMANDS (INCLUDING GUEST VLANS)

The DES-3800 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 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	
create 802.1x guest_vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> | all] state [enable | disable]
delete 802.1x guest_vlan	{<vlan_name 32>}
show 802.1x guest_vlan	

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

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 or Operator-level users can issue this command.

Example usage:

To enable 802.1x switch wide:

```
DES-3800:admin#enable 802.1x
Command: enable 802.1x

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To disable 802.1x on the Switch:

```
DES-3800:admin#disable 802.1x
Command: disable 802.1x

Success.

DES-3800:admin#
```

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 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-3800:admin#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: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE. Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout – Shows the current state of the Backend Authenticator. Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Restrictions	None.

Example usage:

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

```
DES-3800:admin#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-3800:admin#show 802.1x auth_state
Command: show 802.1x auth_state

Port number  :  1
 Index MAC Address        Auth PAE State  Backend State  Port Status
 ----  -----------        --------------- -------------  ----------
 1     00-08-02-4E-DA-FA  Authenticated   Idle           Authorized
 2
 3
 4
 5
 6
 7
 8
 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]* – The Switch allows users to authenticate 802.1x by either port or MAC address.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure 802.1x authentication by MAC address:

```
DES-3800:admin#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DES-3800:admin#
```

config 802.1x capability ports

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

Example usage:

To configure 802.1x capability on ports 1-10:

```
DES-3800:admin#config 802.1x capability ports 1 – 10
authenticator
Command: config 802.1x capability ports 1 – 10
authenticator

Success.

DES-3800:admin#
```

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 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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#config 802.1x auth_parameter ports 1–20
direction both
Command: config 802.1x auth_parameter ports 1–20 direction
both
```

```
Success.

DES-3800:admin#
```

config 802.1x init

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

Example usage:

To initialize the authentication state machine of all ports:

```
DES-3800:admin# config 802.1x init
port_based ports all
Command: config 802.1x init port_based ports
all

Success.

DES-3800:admin#
```

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-

config 802.1x reauth	
	authorized.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-18:

```
DES-3800:admin#config 802.1x reauth port_based ports
1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

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-3800:admin#config radius delete 1
Command: config radius delete 1

Success.

DES-3800:admin#
```

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-3800:admin#config radius 1 10.48.74.121 key
dlink default
Command: config radius 1 10.48.74.121 key dlink
default

Success.
```

```
DES-3800:admin#
```

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	Only Administrator-level users can issue this command.

Example usage:

To display RADIUS settings on the Switch:

```
DES-3800:admin#show radius
Command: show radius

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

Total Entries : 3

DES-3800:admin#
```

create 802.1x guest_vlan

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

Example usage:

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

```
DES-3800:admin#create 802.1x guest_vlan Trinity
Command: create 802.1x guest_vlan Trinity

Success.
```

```
DES-3800:admin#
```

config 802.1x guest_vlan ports

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

Example usage:

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

```
DES-3800:admin#config 802.1x guest_vlan ports 1-5 state
enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DES-3800:admin#
```

show 802.1x guest_vlan

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

Example usage:

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

```
DES-3800:admin#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

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

Success.

DES-3800:admin#
```

delete 802.1x guest_vlan

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

Example usage:

To delete a previously created 802.1x Guest VLAN.

```
DES-3800:admin#delete 802.1x guest_vlan Trinity
Command: delete 802.1x guest_vlan Trinity

Success.

DES-3800:admin#
```

19

ACCESS CONTROL LIST (ACL) COMMANDS

The xStack DES-3800 switch series implements Access Control Lists that enable the Switch to deny or permit network access to specific devices or device groups based on IP settings, MAC address, and packet content.

Command	Parameters
create access_profile	[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-xffff>} | protocol_id {user _mask <hex 0x0-0xffffffff> }]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}}] ipv6 { class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> } [profile_id <value 1-255>]
delete access_profile profile_id	[profile_id <value 1-255> | all]
config access_profile profile_id	<value 1-255> [add access_id [auto_assign | <value 1-65535>] [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> } | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {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-xffffffff> <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 | mirror] | delete access_id <value 1-65535>] ipv6 { class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr> }
show access_profile	profile_id <value 1-255>
show current_config access_profile	
config flow_meter profile_id	<value 1-255> access_id <value 1-65535> rate <value 0-999936> rate_exceed [drop | set_drop_precedence]
show flow_meter	meter { profile_id < value 1-255 > { access_id < access_id >}}
create cpu access_profile	[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 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 {user_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset 16-31 <hex 0x0-0xffffffff> <hex

Command	Parameters
	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>]
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> | ethernet_type <hex 0x0-0xffff>} [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>}]} [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>} [permit | deny] | delete access_id <value 1-65535>]
enable cpu interface_filtering	
disable cpu_interface_filtering	
show cpu_interface_filtering	
show cpu access_profile	{profile_id <value 1-5> {access_id <value 1-65535>}}

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

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

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1

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

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

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

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

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

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

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.

In order to address this functional limitation of the chip set, an additional function, **CPU Interface Filtering**, has been added. CPU Filtering may be universally enabled or disabled. Setting up CPU Interface Filtering follows the same syntax as ACL configuration and requires some of the same input parameters. To configure CPU Interface Filtering, see the descriptions below for **create cpu access_profile** and **config cpu access_profile**. To enable CPU Interface Filtering, see **config cpu_interface_filtering**. The xStack DES-3800 switch series has three ways of creating access profile entries on the Switch which include **Ethernet** (MAC Address), **IP**, and **Packet Content**. Due to the present complexity of the access profile commands, it has been decided to split this command into three pieces to be better understood by the user and therefore simpler for the user to configure. The beginning of this section displays the **create access_profile** and **config access_profile** commands in their entirety. The following table divides these commands up into the defining features necessary to properly configure the access profile. Remember these are not the total commands but the easiest way to implement Access Control Lists for the Switch.

Command	Parameters
create access_profile	[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} profile_id <value 1-255>]
config access_profile profile_id	<value 1-255> [add access_id [auto_assign | <value 1-65535>] [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} port <portlist> [permit {priority <value 0-7> {replace_priority} | deny | mirror] delete <value 1-65535>]
create access_profile	ip [vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-xffff>} | protocol_id {user _mask <hex 0x0-0xffffffff>}]} profile_id <value 1-255>]
config access_profile profile_id	<value 1-255> [add access_id [auto_assign | <value 1-65535>] 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> [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63>} | deny | mirror] delete <value 1-65535>]
create access_profile	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>}
config access_profile profile_id	<value 1-255> [add access_id [auto_assign | <value 1-65535>] packet_content {offset_0-15 <hex0x0-0xffffffff> <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>

Command	Parameters
	<hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex0x0-0xffffffff>} port <portlist> [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63>} | deny | mirror] delete <value 1-65535>]
create access_profile	profile_id <value 1-8> ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]
config access_profile profile_id	<value 1-8> add access_id <value 1-65535> ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destionation_ipv6 <ipv6addr>} port <port> [permit {priority <value 0-7> {replace_priority}} | deny] | delete <value 1-65535>]

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 up 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 tabled below provide a summary of the maximum ACL profile rule limits.

DES-3828/DES-3828DC/DES-3828P

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
51(Gigabit)	100
52(Gigabit)	100
Total Rules	800

DES-3852

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

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.

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

create access_profile (for Ethernet)

Purpose	Used to create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered can 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} profile_id <value 1-255>]**
Description	This command will allow the user to create a profile for packets that may be accepted, denied or mirrored by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the **config access_profile** command for Ethernet, as stated below.
Parameters	*ethernet* - Specifies that the Switch will examine the layer 2 part of each packet header with emphasis on one or more of the following: • *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 the following hexadecimal format: 000000000000-FFFFFFFFFFFF • *destination_mac <macmask>* – Specifies a MAC address mask for the destination MAC address in the following format: 000000000000-FFFFFFFFFFFF • *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. *profile_id <value 1-255>* - Specifies an index number between 1 and 255 that will identify the access profile being created with this command.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create a Ethernet access profile:

```
DES-3800:admin#create access_profile ethernet vlan 802.1p profile_id 1
Command: create access_profile ethernet vlan 802.1p profile_id 1

Success.

DES-3800:admin#
```

config access_profile profile_id (for Ethernet)

Purpose	Used to configure the Ethernet access profile on the Switch and to define specific values for the rules that will be used to by the Switch to determine if a given packet should be forwarded, filtered or mirrored. 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.
Syntax	**config access_profile profile_id <value 1-255> [add access_id [auto_assign | <value 1-65535> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} port <port> [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63> } | deny | mirror] delete <value 1-65535>]**

config access_profile profile_id (for Ethernet)

Description

This command is used to define the rules used by the Switch to either forward, filter or mirror packets based on the Ethernet part of each packet header.

Parameters

profile_id <value 1-255> - Enter an integer between 1 and 255 that is used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given.

add access_id - Adds an additional rule to the above specified access profile.

- *auto_assign* – Adding this parameter will automatically assign an access_id to identify the rule.
- *<value 1-65535>* - The value specifies the relative priority of the additional rule. Up to 65535 different rules may be configured for the Ethernet access profile.

ethernet - Specifies that the Switch will look only into the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following:

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only this previously created VLAN.
- *source_mac <macaddr>* – Specifies that the access profile will apply to only packets with this source MAC address. MAC address entries may be made in the following format: **000000000000-FFFFFFFFFFFF**
- *destination_mac <macaddr>* – Specifies that the access profile will apply to only packets with this destination MAC address. MAC address entries may be made in the following format: **000000000000-FFFFFFFFFFFF**
- *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.

port <portlist> - The access profile for Ethernet may be defined for each port on the Switch by entering a port or range of ports here. Up to 65535 rules may be configured for each port.

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

- *priority <value 0-7>* – This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
- *{replace_priority}* – Enter this parameter if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

replace_dscp <value 0-63> – Allows you to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.

deny – Specifies that packets that match the access profile are not permitted to be forwarded by the Switch and will be filtered.

mirror - Selecting *mirror* specifies that packets that match the access profile are mirrored to a port defined in the **config mirror port** command. Port Mirroring must be enabled and a target port must be set. Remember, Port Mirroring cannot cross-box, that is they cannot span across switches in a switch stack.

config access_profile profile_id (for Ethernet)

delete access_id <value 1-65535> – Use this command to delete a specific rule from the Ethernet profile. Up to 65535 rules may be specified for the Ethernet access profile.

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

Example usage:

To configure a rule for the Ethernet access profile:

```
DES-3800:admin#config access profile profile_id 1 add access_id 1
ethernet vlan Trinity 802.1p 1 port 1 permit priority 1 replace
priority
Command: config access profile profile_id 1 add access_id 1
ethernet vlan Trinity 802.1p 1 port 1 permit priority 1 replace
priority

Success.

DES-3800:admin#
```

create access_profile (IP)

Purpose Used to create an access profile on the Switch by examining the IP part of the packet header. Masks entered can 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 ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-xffff>} | protocol_id_mask {user_define_mask <hex 0x0-0xffffffff> <hex 0x0-0xffffffff><hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]} profile_id <value 1-255>}**

Description This command will allow the user to create a profile for packets that may be accepted, denied or mirrored by the Switch by examining the IP part of the packet header. Specific values for rules pertaining to the IP part of the packet header may be defined by configuring the **config access_profile** command for IP, as stated below.

Parameters *ip* - Specifies that the Switch will look into the IP fields in each packet with special emphasis on one or more of the following:

- *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.

create access_profile (IP)

	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 User 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* – Specifies that the Switch will examine each frame's Protocol ID field. ***user_define_mask <hex 0x0-0xffffffff>*** **– Enter a hexidecimal value that will identify the protocol to be discovered in the packet header.** *profile_id <value 1-255>* - Specifies an index number between 1 and 255 that will identify the access profile being created with this command.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure a rule for the IP access profile:

```
DES-3800:admin#create access_profile ip protocol_id
profile_id 2
Command: create access_profile ip protocol_id profile_id 2

Success.

DES-3800:admin#
```

config access_profile profile_id (IP)

Purpose	Used to configure the IP access profile on the Switch and to define specific values for the rules that will be used to by the Switch to determine if a given packet should be forwarded, filtered or mirrored. 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.
Syntax	**config access_profile profile_id <value 1-255> [add access_id [auto_assign | <value 1-65535>] 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-**

config access_profile profile_id (IP)

0xffffffff><hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}]} port <port> [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63>} | deny | mirror] delete <value 1-65535>]

Description

This command is used to define the rules used by the Switch to either forward, filter or mirror packets based on the IP part of each packet header.

Parameters

profile_id <value 1-255> - Enter an integer between 1 and 255 that is used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given.

add access_id - Adds an additional rule to the above specified access profile.

- *auto_assign* – Adding this parameter will automatically assign an access_id to identify the rule.
- *<value 1-65535>* - The value specifies the relative priority of the additional rule. Up to 65535 different rules may be configured for the Ethernet access profile.

ip – Specifies that the Switch will look into the IP fields in each packet to see if it will be either forwarded or filtered based on one or more of the following:

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only to 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 defined by a value between 0 and 255.
  - *code <value 0-255>* – Specifies that the access profile will apply to this ICMP code defined by a value between 0 and 255.
- *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 defined by a value between 0 and 255.
- *tcp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.
  - *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.
  - *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.
- *flag_mask* – Enter the type of TCP flag to be masked. The choices are:
  - *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 User 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.

config access_profile profile_id (IP)

    - *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 appropriate rules.
    - *user_define <hex 0x0-0xfffffff>* – Enter a hexidecimal value that will identify the protocol to be discovered in the packet header.

port <portlist> - The access profile for IP may be defined for each port on the Switch. Up to 65535 rules may be configured for each port.

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

- *priority <value 0-7>* – This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine to which CoS queue packets are forwarded. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
- *{replace_priority}* – Enter this parameter to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

replace_dscp <value 0-63> – Allows you to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.

deny – Specifies that packets that match the access profile are not permitted to be forwarded by the Switch and will be filtered.

mirror - Selecting *mirror* specifies that packets that match the access profile are mirrored to a port defined in the **config mirror port** command. Port Mirroring must be enabled and a target port must be set. Remember, Port Mirroring cannot cross-box, that is they cannot span across switches in a switch stack.

delete access_id <value 1-65535> – Use this command to delete a specific rule from the IP profile. Up to 65535 rules may be specified for the IP access profile.

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

Example usage:

To configure a rule for the IP access profile:

```
DES-3800:admin#config access_profile profile_id 2 add
access_id 2 ip protocol_id 2 port 1 deny
Command: config access_profile profile_id 2 add
access_id 2 ip protocol_id 2 port 1 deny

Success.

DES-3800:admin#
```

create access_profile (packet content mask)

Purpose Used to create an access profile on the Switch by examining the Ethernet part of the packet header. Packet content masks entered will specify certain bytes of the packet header to be identified by the Switch. When the Switch recognizes a packet with the identical byte as the one configured, it will either forward, filter or mirror the packet, based on the users command. Specific values for the rules are entered using the **config access_profile** command, below.

Syntax **create access_profile packet_content_mask {offset_0-15 <hex 0x0-0xffffffff>**

create access_profile (packet content mask)	
	<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>}
Description	This command is used to identify packets by examining the Ethernet packet header, by byte and then decide whether to filter or forward it, based on the user's configuration. The user will specify which bytes to examine by entering them into the command, in hex form, and then selecting whether to forward, filter or mirror them, using the **config access_profile** command.
Parameters	*packet_content_mask* – Allows users to examine any specified content up to 80 bytes within a packet at one time and 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. With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), D-Link xStack switch family can effectively mitigate some network attacks like the common ARP Spoofing attack widely spreading today. This is for the reason that Packet Content ACL is able to inspect any specified content of a packet in different protocol layers. *profile_id <value 1-255>* - Specifies an index number between 1 and 255 that will identify the access profile being created with this command.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create an Access profile by packet content mask:

```
DES-3800:admin#create access_profile packet_content_mask
offset_0-15 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF
offset_16-31 0xFFFF 0xFFFF0000 0xF 0xF000000 profile_id 3
Command: create access_profile packet_content_mask offset_0-15
0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF offset_16-31
0xFFFF 0xFFFF0000 0xF 0xF000000 profile_id 3

Success.

DES-3800:admin#
```

config access_profile profile_id (packet content mask)	
Purpose	To configure the rule for a previously created access profile command based on the packet content mask. Packet content masks entered will specify certain bytes of the packet header to be identified by the Switch. When the Switch recognizes a packet with the identical byte as the one configured, it will either forward, filter or mirror the packet, based on the users command entered here.
Syntax	**config access_profile profile_id <value 1-8> [add access_id <value 1-65535> packet_content_mask {offset_0-15 <hex0x0-0xffffffff> <hex 0x0-0xffffffff>**

config access_profile profile_id (packet content mask)

<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> <hex0x0-0xffffffff>} port <port> [permit {priority <value 0-7> {replace_priority} | replace_dscp <value 0-63> } | deny | mirror] delete access_id <value 1-65535>]

Description

This command is used to set the rule for a previously configured access profile setting based on packet content mask. These rules will determine if the Switch will forward, filter or mirror the identified packets, based on user configuration specified in this command. Users will set bytes to identify by entering them in hex form, offset from the first byte of the packet.

Parameters

profile_id <value 1-255> - Enter an integer between 1 and 255 that is used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given.

add access_id - Adds an additional rule to the above specified access profile.

- *auto_assign* – Adding this parameter will automatically assign an access_id to identify the rule.
- *<value 1-65535>* - The value specifies the relative priority of the additional rule. Up to 65535 different rules may be configured for the Ethernet access profile.

packet_content – Allows users to examine any specified content up to 80 bytes within a packet at one time and 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. With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), D-Link xStack switch family can effectively mitigate some network attacks like the common ARP Spoofing attack widely spreading today. This is for the reason that Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

port <portlist> - The access profile for the packet content mask may be defined for each port on the Switch. Up to 65535 rules may be configured for each port.

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

- *priority <value 0-7>* – This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
- *{replace_priority}* – Enter this parameter if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

replace_dscp <value 0-63> – Allows you to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part

config access_profile profile_id (packet content mask)	
	of the command. This value will over-write the value in the DSCP field of the packet. *deny* – Specifies that packets that match the access profile are not permitted to be forwarded by the Switch and will be filtered. *mirror* - Selecting *mirror* specifies that packets that match the access profile are mirrored to a port defined in the **config mirror port** command. Port Mirroring must be enabled and a target port must be set. Remember, Port Mirroring cannot cross-box, that is they cannot span across switches in a switch stack. *delete access_id <value 1-65535>* – Use this command to delete a specific rule from the packet content mask profile. Up to 65535 rules may be specified for the Packet Content access profile.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create an access profile by packet content mask:

```
DES-3800:admin# config access_profile profile_id 3 add access_id 1
packet_content offset_0-15 0x11111111 0x11111111 0x11111111
0x11111111 offset_16-31 0x11111111 0x11111111 0x11111111 0x11111111
port 1 deny
Command: config access_profile profile_id 3 add access_id 1
packet_content offset_0-15 0x11111111 0x11111111 0x11111111
0x11111111 offset_16-31 0x11111111 0x11111111 0x11111111 0x11111111
port 1 deny

Success.

DES-3800:admin#
```

NOTE: Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC Address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN (known as ARP spoofing attack). For a more detailed explaination on how ARP protocol works and how to employ D-Link’s advanced unique Packet Content ACL to prevent ARP spoofing attack, please see Appendix B, at the end of this manual.

create access_profile (ipv6)	
Purpose	Used to create an access profile on the Switch by examining the IPv6 part of the packet header. 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 ipv6 profile_id <value 1-8> {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]**
Description	This command is used to identify various parts of IPv6 packets that enter the Switch so they can be forwarded, filtered or mirrored.
Parameters	*profile_id <value 1-8>* - Specifies an index number between 1 and 8 that will identify the access profile being created with this command. *ipv6* – Denotes that IPv6 packets will be examined by the Switch for forwarding or filtering based on the rules configured in the **config access_profile** command for IPv6. IPv6 packets may be identified by the following: • *class* – Entering this parameter will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4. • *flowlabel* – Entering this parameter will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets. • *source_ipv6_mask <ipv6mask>* - Specifies an IP address mask for the source IPv6 address. • *destination_ipv6_mask <ipv6mask>* - Specifies an IP address mask for the destination IPv6 address.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create an access profile based on IPv6 classification:

```
DES-3800:admin# create access_profile ipv6 class
flowlabel profile_id 4
Command: create access_profile ipv6 class flowlabel
profile_id 4

Success.

DES-3800:admin#
```

config access_profile profile_id (ipv6)	
Purpose	Used to configure the IPv6 access profile on the Switch and to define specific values for the rules that will be used to by the Switch to determine if a given packet should be forwarded, filtered or mirrored. 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.
Syntax	**config access_profile profile_id <value 1-8> [add access_id <value 1-65535>] ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destionation_ipv6 <ipv6addr>} port <port> [permit {priority <value 0-7> {replace_priority}} | deny] | delete <value 1-65535>]**
Description	This command is used to define the rules used by the Switch to either filter, forward or mirror packets based on the IPv6 part of each packet header.
Parameters	*profile_id <value 1-8>* - Enter an integer between 1 and 8 that is used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the create access_profile command. The lower the profile ID, the higher the priority the rule will be given. *add access_id <value 1-65535>* - Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 65535 different rules may be configured for the IPv6 access profile. *ipv6* - Specifies that the Switch will look into the IPv6 fields in each packet, with emphasis on one or more of the following fields: • *class <value 0-255>* - Entering this parameter will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4. • *flowlabel <hex 0x0-fffff>* - Entering this parameter will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets. This field is to be defined by the user in hex form. • *source_ipv6 <ipv6addr>* - Specifies an IP address mask for the source IPv6 address. • *destination_ipv6 <ipv6addr>* - Specifies an IP address mask for the destination IPv6 address. *port <portlist>* - The access profile for Ethernet may be defined for each port on the Switch. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are

config access_profile profile_id (ipv6)	
	specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *permit* – Specifies that packets that match the access profile are permitted to be forwarded by the Switch. • *priority <value 0-7>* – This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. • *{replace_priority}* – Enter this parameter to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. *deny* – Specifies that packets that match the access profile are not permitted to be forwarded by the Switch and will be filtered. *delete access_id <value 1-65535>* – Use this command to delete a specific rule from the IPv6 profile. Up to 65535 rules may be specified for the IPv6 access profile.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure a previously created access profile based on IPv6 classification:

```
DES-3800:admin# config access_profile profile_id 4 add
access_id 1 ipv6 class 1 flowlabel 0xABCD port 1:4 deny
Command: config access_profile profile_id 4 add
access_id 1 ipv6 class 1 flowlabel 0xABCD port 1:4 deny

Success.

DES-3800:admin#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile profile_id [<value 1-255> | all]**
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. *all* – Entering this parameter will delete all access profiles currently configured on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DES-3800:admin#
```

show access_profile

Purpose	Used to display the currently configured access profiles on the Switch.
Syntax	**show access_profile {profile_id <value 1-255>}**
Description	The **show access_profile** command is used to display the currently configured access profiles.
Parameters	*profile_id <value 1-255>* – Enter an integer between 1 and 255 that is used to identify the access profile that will be viewed with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. Entering this command without the *profile_id* parameter will command the Switch to display all access profile entries.
Restrictions	None.

Example usage:

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

```
DES-3800:admin#show access_profile
Command: show access_profile


Access Profile Table

Access Profile ID: 1                   TYPE : Ethernet
======================================================================
Owner         : ACL
Masks         :
VLAN
-----------------------

Access ID   : 1             Mode: Permit
```

```
Owner         : ACL
Ports           : 10
-----------  ------
Trinity      1
======================================================================
Access Profile ID: 2                   TYPE : IP
======================================================================
Owner         : ACL
Masks         :
VLAN
--------------------

Access ID : 1                Mode :  Permit
Owner     : ACL
Port      : 10
---------------------
default
======================================================================
Access Profile ID: 3                   TYPE : Packet Content
======================================================================
Owner        : ACL
Masks        :
Offset  0-15 : 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF
Offset 16-31 : 0x0000FFFF 0xFFFF0000 0x0000000F 0x0F000000

Access ID : 1              Mode: Deny
Owner     : ACL
Port      : 10
======================================================================
Access Profile ID: 10                  TYPE : IPV6
======================================================================
Owner         : ACL
Masks         :
Class          Flow Label          Source IPv6
-----------    -------------------  -----------------------------------
                                     FFFF: :FFFF
                                     Dst.  Ipv6 Mask
                                    -----------------------------------
                                     FFFF: :FFFF

Access ID : 1                Mode :  Permit
Owner     : ACL
Port      : 10
--------- -----            -------------------------------------------
100       0x1234           1122:3344
                           5566:7788

======================================================================
ACL Free: System : 796, Port 1-8 : 200, Port 9-16 : 196, Port 17-24:200
          Port 25 :  100, Port 26  : 100, Port 27 : 100, Port 28:  100

Total Access Entries: 4

DES-3800:admin#
```

show current_config access_profile

Purpose	Used to show the ACL CLI commands in current configuration.
Syntax	show current_config access_profile
Description	The ACL port will be displayed by this command.
Parameters	None.
Restrictions	None.

Example usage:

To display ACL part:

```
DES-3800:admin#show current_config access_profile
Command: show current_config access_profile

#-------------------------------------------------------------

# ACL

create access_profile ethernet vlan profile_id 1
config access_profile profile_id 1 add access_id 1 ethernet vlan default
port 1
permit
disable cpu_interface_filtering

#-------------------------------------------------------------

DES-3800:admin#
```

config flow_meter

Purpose	To configure packet flow-based metering based on an access profile and rule.
Syntax	config flow_meter profile_id <value 1-255> access_id <value 1-65535> rate <value 0-999936> rate_exceed [drop | set_drop_precedence]
Description	This command is used to configure the flow-based metering function, users may set the preferred bandwidth for this rule, in Kbps and once the bandwidth has been exceeded, overflow packets will be either dropped or be set for a drop precedence, depending on user configuration. The set_drop_precedence function work with WRED. Note: If the bandwidth is configured as zero, the meter will be destroyed.
Parameters	*Profile_id* - Specifies the profile_ID *access_id* - Specifies the access_ID *Rate* - Specify the committed bandwidth in Kbps for the flow. The value of 0 means to delete this flow_meter setting. *rate_exceed* - This specifies the action for packet which exceed the committed rate.The action can be specified to be one of the following. *drop_packet*: drop_packet. *set_drop_precedence*: the packet will not be dropped right away. However, when the traffic is busy, it has the higher probability to be dropped in the

config flow_meter

	later stage.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage: To configure the flow meter:

```
DES-3800:admin#config flow_meter profile_id 1 access_id 1  rate
64232 rate_exceed drop
Command:config flow_meter profile_id 1 access_id 1  rate 64232
rate_exceed drop
Success
DES-3800:admin#
```

show flow_meter

Purpose	Used to display the flow-based metering configuration.
Syntax	show flow_meter {profile_id < value 1-255 > { access_id < access_id >}}
Description	This command displays the flow meter configuration.
Parameters	*Profile_id* - Specifies the profile_ID *access_id* - Specifies the access_ID
Restrictions	None.

Example usage: To display the flow meter:

```
DES-3800:admin#show flow_meter
Command: show flow_meter

Flow Meter information:
Profile ID   Access ID   Metering Rate(Kbps)   Rate Exceed Action
----------   ---------   ------------------    ------------------
1            1           192                   drop_packet
Total Flow Meter Entries: 1

DES-3800:admin#
```

20

TRAFFIC SEGMENTATION COMMANDS

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

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

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

config traffic_segmentation

Purpose	Used to configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation <portlist> forward_list [null | <portlist>]**
Description	The **config traffic_segmentation** command is used to configure traffic segmentation on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports that will be configured for traffic segmentation. *forward_list* – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above. • *null* – No ports are specified • *<portlist>* – Specifies a range of ports for the forwarding list. This list must be on the same Switch previously specified for traffic segmentation (i.e. following the *<portlist>* specified above for config traffic_segmentation).
Restrictions	Only Administrator or Operator-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-3800:admin# config traffic_segmentation 1-10
forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list
11-15

Success.

DES-3800:admin#
```

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	None. 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-3800:admin#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

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

21

COMMAND LIST HISTORY

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

Command	Parameters
?	{<command>}
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-3800:admin#?

..
?
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 capability ports
config 802.1x guest_vlan
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config address_binding ip_mac ipaddress
config address_binding ip_mac ports
config admin local_enable

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

To display the parameters for a specific command:

```
DES-3800:admin#? 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-3800:admin#
```

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-3800:admin#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 capability ports
config 802.1x guest_vlan
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config address_binding ip_mac ipaddress
config address_binding ip_mac ports
config admin local_enable
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	Only Administrator-level users can issue this command.

Example usage

To configure the command history:

```
DES-3800:admin#config command_history 20
Command: config command_history 20

Success.

DES-3800:admin#
```

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-3800:admin#show command_history
Command: show command_history

?
? show
show vlan
show command history

DES-3800:admin#
```

22

BASIC IP COMMANDS (FOR LAYER 3)

IP Multinetting is a function that allows multiple IP interfaces to be assigned to the same VLAN. This is beneficial to the administrator when the number of IPs on the original interface is insufficient and the network administrator wishes not to resize the interface. IP Multinetting is capable of assigning another IP interface on the same VLAN without affecting the original stations or settings of the original interface.

Two types of interfaces are configured for IP multinetting, *primary* and *secondary*, and every IP interface must be classified as one of these. A *primary* interface refers to the first interface created on a VLAN, with no exceptions. All other interfaces created will be regarded as *secondary* only, and can only be created once a *primary* interface has been configured. There may be five interfaces per VLAN (one primary, and up to four secondary) and they are, in most cases, independent of each other. *Primary* interfaces cannot be deleted if the VLAN contains a *secondary* interface. Once the user creates multiple interfaces for a specified VLAN (*primary* and *secondary*), that set IP interface cannot be changed to another VLAN.

IP Multinetting is a valuable tool for network administrators requiring a multitude of IP addresses, but configuring the Switch for IP multinetting may cause troubleshooting and bandwidth problems, and should not be used as a long term solution. Problems may include:

The Switch may use extra resources to process packets for multiple IP interfaces.

The amount of broadcast data, such as RIP update packets and PIM hello packets, will be increased

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

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

Command	Parameters
create ipif	<ipif_name 12> <ip_addr/netmask> <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable]}
config ipif	<ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | proxy_arp [enable | disable]} | bootp | dhcp]
enable ipif	{<ipif_name 12> | all}
disable ipif	{<ipif_name 12> | all}
delete ipif	{<ipif_name 12> | all}
show ipif	{<ipif_name 12>}

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

create ipif	
Purpose	Used to create an IP interface on the Switch.
Syntax	**create ipif <ipif_name 12> <ip_addr/netmask> <vlan_name 32> {secondary | {state [enable | disable] | proxy_arp [enable | disable]}**
Description	This command will create an IP interface.
Parameters	*<ipif_name 12>* – The name for the IP interface to be created. The user may enter an alphanumeric string of up to 12 characters to define the IP interface. *<ip_addr/netmask>* – IP address and netmask of the IP interface to be created. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0) or in CIDR format, (10.1.2.3/8). (This parameter may also appear as <ip_addr/netmask>). *<vlan_name 32>* – The name of the VLAN that will be associated with the above IP interface. *secondary* – Enter this parameter if this configured IP interface is to be a *secondary* IP interface of the VLAN previously specified. *secondary*

create ipif

	interfaces can only be configured if a *primary* interface is first configured. *proxy_arp [enable | disable]* – Choose to enable or disable the proxy ARP for this IP interface. The Proxy ARP feature will allow this IP interface to reply to ARP requests destined for another interface by faking its identities the original ARP requester. The Switch is then capable of routing packets to the intended destination without configuring static routing or a default gateway. The default is disable. *state [enable | disable]* – Allows the user to enable or disable the IP interface.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create the primary IP interface, P1-1 on VLAN Trinity:

```
DES-3800:admin#create ipif p1 ipaddress 10.1.1.1 Trinity state
enable
Command: create ipif p1 ipaddress 10.1.1.1 Trinity state enable

Success.

DES-3800:admin#
```

To create the secondary IP interface, P1-1 on VLAN Trinity:

```
DES-3800:admin#create ipif p1-1 ipaddress 12.1.1.1 Trinity
secondary state enable
Command: create ipif p1-1 ipaddress 12.1.1.1 Trinity secondary
state enable

Success.

DES-3800:admin#
```

config ipif

Purpose	Used to configure an IP interface set on the Switch.
Syntax	**config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable] | proxy_arp [enable | disable]} | bootp | dhcp]**
Description	This command is used to configure the System IP interface on the Switch.
Parameters	*<ipif_name 12>* - Enter the previously created IP interface name desired to be configured. *ipaddress <network_address>* – IP address and netmask of the IP interface to be configured. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). (This parameter may also appear as <ip_addr/netmask>). *vlan <vlan_name 32>* – The name of the VLAN corresponding to the previously created IP interface. If a primary and secondary IP interface are configured for the same VLAN (subnet), the user cannot change the VLAN of the IP interface. *state [enable | disable]* – Allows users to enable or disable the IP interface. *proxy_arp [enable | disable]* – Choose to enable or disable the proxy

config ipif	
	ARP for this IP interface. The Proxy ARP feature will allow this IP interface to reply to ARP requests destined for another interface by faking its identities the original ARP requester. The Switch is then capable of routing packets to the intended destination without configuring static routing or a default gateway. The default is disable. *bootp* – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch’s System IP interface. *dhcp* – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch’s System IP interface.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DES-3800:admin#config ipif System ipaddress
10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DES-3800:admin#
```

enable ipif	
Purpose	Used to enable an IP interface on the Switch.
Syntax	**enable ipif {<ipif_name 12> | all}**
Description	This command will enable the IP interface function on the Switch.
Parameters	*<ipif_name 12>* – The name of a previously configured IP interface to enable. Enter an alphanumeric entry of up to twelve characters to define the IP interface. *all* – Entering this parameter will enable all the IP interfaces currently configured on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the ipif function on the Switch:

```
DES-6500:4#enable ipif s2
Command: enable ipif s2

Success.

DES-6500:4#
```

disable ipif	
Purpose	Used to disable the configuration of an IP interface on the Switch.
Syntax	**disable ipif {<ipif_name 12> | all}**
Description	This command will disable an IP interface on the Switch, without altering its configuration values.
Parameters	*<ipif_name 12>* – The name previously created to define the IP interface.

disable ipif

	all – Entering this parameter will disable all the IP interfaces currently configured on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable the IP interface named “s2”:

```
DES-3800:admin#disable ipif s2
Command: disable ipif s2

Success.

DES-3800:admin#
```

delete ipif

Purpose	Used to delete the configuration of an IP interface on the Switch.
Syntax	**delete ipif {<ipif_name 12> | all}**
Description	This command will delete the configuration of an IP interface on the Switch.
Parameters	*<ipif_name 12>* – The name of the IP interface to delete. *all* – Entering this parameter will delete all the IP interfaces currently configured on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete the IP interface named s2:

interface named “s2”:

```
DES-3800:admin# delete ipif s2
Command: delete ipif s2

Success.

DES-3800:admin#
```

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 to be viewed.
Restrictions	None.

Example usage:

To display IP interface settings.

```
DES-3800:admin#show ipif System
Command: show ipif System
```

```
IP Interface Settings

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

Total Entries : 1

DES-3800:admin#
```

NOTE: In the IP Interface Settings table shown above, the Secondary field will have two displays. *FALSE* denotes that the IP interface is a primary IP interface while *TRUE* denotes a secondary IP interface.

23

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}
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 or Operator-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-3800:admin#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-3800:admin#
```

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 or Operator-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-3800:admin#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-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To configure ARP aging time:

```
DES-3800:admin#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-3800:admin#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	**show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static}**
Description	This command is used to display the current contents of the Switch's ARP table.
Parameters	*ipif <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.
Restrictions	None.

Example usage:

To display the ARP table**:**

```
DES-3800:admin#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     10.9.68.1       00-A0-C9-A4-22-5B  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 = 4

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To remove dynamic entries in the ARP table:

```
DES-3800:admin#clear arptable
Command: clear arptable

Success.

DES-3800:admin#
```

24

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 | <network_address>] <ipaddr> {<metric 1-65535>}{[primary | backup]}
delete iproute default	<ipaddr>
delete iproute	delete iproute [default | <network_address>] {[primary | backup]}
show iproute	{<network_address> | rip | ospf}
show iproute static	
config iproute ospf ecmp	[enable | disable]

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

create iproute

Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	**create iproute [default | <network_address>] <ipaddr> {<metric 1-65535>}{[primary | backup]}**
Description	This command is used to create a primary and backup IP route entry to the Switch's IP routing table.
Parameters	*<network_address>* – IP address and netmask of the IP interface that is the destination of the route. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *<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. *[primary | backup]* - The user may choose between Primary and Backup. If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To add a single static address 10.48.74.121, mask 255.0.0.0 and gateway 10.1.1.254 to the routing table:

```
DES-3800:admin#create iproute 10.48.74.121/255.0.0.0
10.1.1.254 1
Command: create iproute 10.48.74.121/8 10.1.1.254 1

Success.

DES-3800:admin#
```

delete iproute

Purpose	Used to delete an IP route entry from the Switch’s IP routing table.
Syntax	**delete iproute [default | <network_address>] {[primary | backup]}**
Description	This command will delete an existing entry from the Switch’s IP routing table.
Parameters	*<network_address>* – IP address and netmask of the IP interface that is the destination of the route. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *<ipaddr>* – The gateway IP address for the next hop router. [*primary* | *backup]* – The user may choose between Primary and Backup. If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete a backup static address 10.48.75.121, mask 255.0.0.0 and gateway (ipaddr) entry of 10.1.1.254 from the routing table:

```
DES-3800:admin#delete iproute 10.48.74.121/8
10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254

Success.

DES-3800:admin#
```

show iproute

Purpose	Used to display the Switch’s current IP routing table.
Syntax	**show iproute {<network_address>} {[rip | ospf]}**
Description	This command will display the Switch’s current IP routing table.
Parameters	*<network_address>* –The IP address and netmask of the IP interface that is the destination of the route. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *rip* – Use this parameter to display RIP IP route entries. *ospf* – Use this parameter to display OSPF IP route entries.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DES-3800:admin#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway    Interface   Hops  Protocol
------------------  ---------- ----------- ----- --------
10.0.0.0/8          0.0.0.0    System      1     Local

Total Entries : 1

DES-3800:admin#
```

config iproute ospf ecmp

Purpose	Used to control the OSPF ECMP function.
Syntax	**config iproute ospf ecmp**
Description	This command is used to enable or disable the ECMP function.
Parameters	*enable*- Enables ECMP *disable*- Disables ECMP
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To config the iproute ospf ecmp command:

```
DES-3800:admin#config iproute ospf ecmp enable
Command: config iproute ospf ecmp enable

Success.

DES-3800:admin#
```

25

ROUTE REDISTRIBUTION COMMANDS

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

Command	Parameters
create route redistribute dst ospf src	[static | rip | local] {mettype [1 | 2] | metric <value 0-16777214>}
create route redistribute dst rip src	[local | static | ospf {all | internal | external | type_1 | type_2 | inter+e1| inter+e2}] {metric <value 0-16>}
config route redistribute dst ospf src	[static | rip | local] {mettype [1 | 2] | metric <value 0-16777214>}
config route redistribute dst rip src	[local | static | ospf {all | internal | external | type_1 | type_2 | inter+e1| inter+e2}] {metric <value 0-16>}
delete route redistribute	[dst [rip | ospf] src [rip | static | local | ospf]]
show route redistribute	{dst [rip | ospf] | src [rip | static | local | ospf]}

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

create route redistribute dst ospf src

Purpose	Used to add route redistribution settings for the exchange of RIP routes to OSPF routes on the Switch.
Syntax	**create route redistribute dst ospf src [static | rip| local] {mettype [1 | 2] | metric <value 0-16777214>}**
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local xStack switch is also redistributed.
Parameters	*src [static | rip | local]* – Allows for the selection of the protocol for the source device. *mettype [1 | 2]* – Allows for the selection of one of two methods of calculating the metric value. • Type-1 calculates (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. • Type-2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. *metric <value* 0-16777214> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only Administrator or Operator-level users can issue this command.

Routing information source – RIP. the Static Route table, and the Local interface routing information. Routing information will be redistributed to OSPF.

Route Source	Metric	Metric Type
RIP	0 to 16777214	mettype 1 mettype 2
Static	0 to 16777214	mettype 1 mettype 2
Local	0 to 16777214	mettype 1 mettype 2

Allowed Metric Type combinations are **mettype 1** or **mettype 2**. The metric value **0** above will be redistributed in OSPF as the metric **20**.

Example usage:

To add route redistribution settings:

```
DES-3800:admin#create route redistribute dst ospf
src rip
Command: create route redistribute dst ospf src rip

Success.

DES-3800:admin#
```

create route redistribute dst rip src

Purpose	Used to add route redistribution settings for the exchange of OSPF routes to RIP routes on the Switch.
Syntax	**create route redistribute dst rip src [local | static | ospf {all | internal | external | type_1 | type_2 | inter+e1 | inter+e2}] {metric <value 0-16>}**
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local xStack switch is also redistributed
Parameters	*src* – Allows the selection of the protocol of the source device, as being either local, static or OSPF. After selecting the source device, the user may set the following parameters for that source device from the following options: • *all* – Specifies both internal an external. • *internal* – Specifies the internal protocol of the source device. • *external* - Specifies the external protocol of the source device. • *type_1* - Calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. • *type_2* - Uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. • *inter+e1* – Specifies the internal protocol AND type 1 of the external protocol. • *inter+e2* – Specifies the internal protocol AND type 2 of the external protocol. *metric <value 0-16>* – Allows the entry of an OSPF interface cost. This is analogous to a HOP Count in the RIP routing protocol.
Restrictions	Only Administrator or Operator-level users can issue this command.

Routing information source – OSPF and the Static Route table. Routing information will be redistributed to RIP. The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed.

Route Source	Metric	Type
OSPF	0 to 16	all type_1 type_2 inter+e1 inter+e2 external internal
Static	0 to 16	not applicable

Entering the **Type** combination – **internal type_1 type_2** is functionally equivalent to **all**. Entering the combination **type_1 type_2** is functionally equivalent to **external**. Entering the combination **internal external** is functionally equivalent to **all**.

Entering the metric **0** specifies transparency.

Example usage:

To add route redistribution settings

```
DES-3800:admin#create route redistribute dst rip src ospf
all metric 2
Command: create route redistribute dst rip src ospf all
metric 2

Success.

DES-3800:admin#
```

config route redistribute dst ospf src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the Switch.
Syntax	**config route redistribute dst ospf src [static | rip | local] {mettype [1 | 2] | metric <value 0-16777214>}**
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. This is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	*src [static* | *rip* | *local]* – Allows the selection of the protocol of the source device. *mettype* – allows the selection of one of the methods for calculating the metric value. • Type - 1 calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. • Type - 2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. *metric <value* 0-16777214> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only Administrator or Operator-level users can issue this command.

Routing information source – RIP: the Static Route table, and the Local interface routing information. Routing information will be redistributed to OSPF. The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed.

Route Source	Metric	Metric Type
RIP	0 to 16777214	mettype 1 mettype 2
Static	0 to 16777214	mettype 1 mettype 2
Local	0 to 16777214	mettype 1 mettype 2

Allowed Metric Type combinations are **mettype 1** or **mettype 2**. The metric value **0** above will be redistributed in OSPF as the metric **20**.

Example usage:

To configure route redistributions:

```
DES-3800:admin#config route redistribute dst ospf src
all metric 2
Command: config route redistribute dst ospf src all
metric 2

Success.

DES-3800:admin#
```

config route redistribute dst rip src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the Switch.
Syntax	**config route redistribute dst rip src [local | static | ospf {all | internal | external | type_1 | type_2 | inter+e1 | inter+e2}] {metric <value 0-16>}**
Description	Route redistribution allows routers on the network that are running different routing protocols to exchange routing information. This is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The Switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	*src* - Allows the selection of the protocol of the source device, as being either local, static or OSPF. After selecting the source device, the user may set the following parameters for that source device from the following options: • *all* – Specifies both internal an external. • *internal* – Specifies the internal protocol of the source device. • *external* - Specifies the external protocol of the source device. • *type_1* - Calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. • *type_2* - Uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF.

config route redistribute dst rip src

	• *inter+e1* – Specifies the internal protocol AND type 1 of the external protocol. • *inter+e2* – Specifies the internal protocol AND type 2 of the external protocol. *metric <value 0-16>* – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure route redistributions:

```
DES-3800:admin#config route redistribute dst ospf src rip mettype
type_1 metric 2
Command: config route redistribute dst ospf src rip mettype type_1
metric 2

Success.

DES-3800:admin#
```

delete route redistribute

Purpose	Used to delete an existing route redistribute configuration on the Switch.
Syntax	**delete route redistribute {dst [rip | ospf] src [rip | static | local | ospf]}**
Description	This command will delete the route redistribution settings on this switch.
Parameters	*dst [rip* | *ospf]* – Allows the selection of the protocol on the destination device. The user may choose between RIP and OSPF. *src [rip* | *static* | *local* | *ospf]* – Allows the selection of the protocol on the source device. The user may choose between RIP, static, local or OSPF.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete route redistribution settings:

```
DES-3800:admin#delete route redistribute dst rip
src ospf
Command: delete route redistribute dst rip src
ospf


Success.


DES-3800:admin#
```

show route redistribute

Purpose	Used to display the route redistribution on the Switch.
Syntax	**show route redistribute {dst [rip | ospf] | src [rip | static | local | ospf]}**
Description	Displays the current route redistribution settings on the Switch.
Parameters	*src [rip* | *static* | *local* | *ospf]* – Allows the selection of the routing protocol on the source device. The user may choose between RIP, static, local or OSPF. *dst [rip* | *ospf]* – Allows the selection of the routing protocol on the destination device. The user may choose between RIP and OSPF.
Restrictions	None.

Example usage:

To display route redistributions:

```
DES-3800:admin#show route redistribute
Command: show route redistribute

Destination Source       Type          Metric
Protocol    Protocol
--------    ------------ --------      --------
RIP         STATIC       All           1
OSPF        LOCAL        Type-2        20

Total Entries : 2

DES-3800:admin#
```

26

RIP COMMANDS

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

Command	Parameters
config rip	[ipif <ipif_name 12> | all] {authentication [enable <password 16> | disable] | tx_mode [disable | v1_only | v1_compatible | v2_only] | rx_mode [v1_only | v2_only | v1_or_v2 | disable] state [enable | disable]}
enable rip	
disable rip	
config rip timer	[update_interval <sec 1-65535> | timeout_interval <sec 1-65535> | garbage_collect_interval <sec 1-65535>]
show rip	ipif <ipif_name 12>

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

config rip

Purpose Used to configure RIP on the Switch.

Syntax **config rip [ipif <ipif_name 12> | all] {authentication [enable <password 16> | disable] | tx_mode [disable | v1_only | v1_compatible | v2_only] | rx_mode [v1_only | v2_only | v1_or_v2 | disable] state [enable | disable]}**

Description This command is used to configure RIP on the Switch.

Parameters *<ipif_name 12>* – The name of the IP interface.

all – To configure all RIP receiving mode for all IP interfaces.

authentication [enable | *disable]* – Enables or disables authentication for RIP on the Switch.

- *<password 16>* – Allows the specification of a case-sensitive password.

tx_mode – Determines how received RIP packets will be interpreted – as RIP version *V1 only*, *V2 Only*, or *V1 Compatible (V1 and V2)***.** This entry specifies which version of the RIP protocol will be used to transfer RIP packets. The disabled entry prevents the reception of RIP packets.

- *disable* – Prevents the transmission of RIP packets.
- *v1_only* – Specifies that only RIP v1 packets will be transmitted.
- *v1_compatible* – Specifies that only RIP v1 compatible packets will be transmitted.
- *v2_only* - Specifies that only RIP v2 packets will be transmitted.

rx_mode – Determines how received RIP packets will be interpreted – as RIP version *V1 only, V2 Only*, or *V1 or V2*. This entry specifies which version of the RIP protocol will be used to receive RIP packets. The Disabled entry prevents the reception of RIP packets.

- *v1_only* – Specifies that only RIP v1 packets will be transmitted.
- *v2_only* - Specifies that only RIP v2 packets will be transmitted.
- *v1_or_v2* - Specifies that only RIP v1 or v2 packets will be transmitted.

config rip

	state [enable | *disable]* – Allows RIP to be enabled and disabled on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To change the RIP receive mode for the IP interface System:

```
DES-3800:admin#config rip ipif System rx_mode v1_only
Command: config rip ipif System rx_mode v1_only

Success.

DES-3800:admin#
```

enable rip

Purpose	Used to enable RIP.
Syntax	**enable rip**
Description	This command is used to enable RIP on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable RIP:

```
DES-3800:admin#enable rip
Command: enable rip

Success.

DES-3800:admin#
```

disable rip

Purpose	Used to disable RIP.
Syntax	**disable rip**
Description	This command is used to disable RIP on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable RIP:

```
DES-3800:admin#disable rip
Command: disable rip

Success.

DES-3800:admin#
```

config rip timer

Purpose	Used to configure the timer interval.
Syntax	**config rip timer [update_interval <sec 1-65535> | timeout_interval <sec 1-65535> | garbage_collect_interval <sec 1-65535>]**
Description	This command configure the timer interval.
Parameters	*update_interval* - The update interval in seconds for the update timer which triggers routing updates periodically. The default value is 30. *timeout_interval* - The timeout interval in seconds for the timeout timer. Each route entry has a timeout timer associated with it. When the timeout timer expires, the route is marked invalid but is retained until the garbage-collection timer expires. The default value is 180. *garbage_collect_interval* - The garbage-collection interval in seconds for the garbage-collection timer. When the timeout timer for a route entry expires, this route entry has a garbage-collection timer associated with it. When the garbage-collection timer expires, this route is deleted. The default value is 120.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure all RIP timers:

```
DES-3800:admin#config rip timer update_interval 20
Command: config rip timer update_interval 20


Success.


DES-3800:admin#config rip timer timeout_interval 120
Command: config rip timer timeout_interval 120


Success.


DES-3800:admin#config rip timer
garbage_collect_interval 80
Command: config rip timer garbage_collect_interval 80


Success.


DES-3800:admin#
```

show rip

Purpose	Used to display the RIP configuration and statistics for the Switch.
Syntax	**show rip {ipif <ipif_name 12>}**
Description	This command will display the RIP configuration and statistics for a given IP interface or for all IP interfaces.
Parameters	*ipif <ipif_name 12>* – The name of the IP interface for which to display the RIP configuration and settings. If this parameter is not specified, the **show rip** command will display the global RIP configuration for the Switch.
Restrictions	None.

Example usage:

To display RIP configuration:

```
DES-3800:admin#show rip
Command: show rip

RIP Global State : Disabled
Update Interval : 30 seconds
Timeout Interval : 180 seconds
Garbage-collection Interval : 120 seconds


RIP Interface Settings

Interface     IP Address/Netmask  TX Mode   RX Mode    Authen-   State
State                                                  tication
------------- ---------------    --------  --------   --------  --------
System        10.41.44.33/8       V2 Only   V1 or V2   Disabled  Disabled

Total Entries : 1

DES-3800:admin#
```

Example usage:

To display RIP configurations by IP interface:

```
DES-3800:admin#show rip ipif System
Command: show rip ipif System

RIP Interface Settings

Interface Name: System
IP Address/Netmask: 10.53.13.33/8 (Link Up)
Interface Metric: 1 (Default)
Administrative State: Disabled
TX Mode: V2 Only
RX Mode: V1 or V2
Authentication: Disabled

Total Entries: 1

DES-3800:admin#
```

27

IGMP COMMANDS

IGMP or Internet Group Management Protocol is a protocol implemented by systems utilizing IPv4 to collect the membership information needed by the multicast routing protocol through various query messages sent out from the router or switch. Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP**) is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active.

In the case where there is more than one multicast router on a subnetwork, one router is elected as the 'querier'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given subnetwork or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnetwork. If there are no members on a subnetwork, packets will not be forwarded to that subnetwork.

The current release of the xStack DES-3800 Series switches now implements IGMPv3. Improvements of IGMPv3 over version 2 include:

- The introduction of the *SSM* or *Source Specific Multicast*. In previous versions of IGMP, the host would receive all packets sent to the multicast group. Now, a host will receive packets only from a specific source or sources. This is done through the implementation of *include* and *exclude* filters used to accept or deny traffic from these specific sources.
- In IGMPv2, Membership reports could contain only one multicast group whereas in v3, these reports can contain multiple multicast groups.
- Leaving a multicast group could only be accomplished using a specific leave message in v2. In v3, leaving a multicast group is done through a Membership report which includes a block message in the group report packet.
- For version 2, the host could respond to either a group query but in version 3, the host is now capable to answer queries specific to the group and the source.

IGMPv3 is backwards compatible with other versions of IGMP and all IGMP protocols must be used in conjunction with PIM-DM or DVMRP for optimal use.

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

Command	Parameters
config igmp	[ipif <ipif_name 12> | all] {version <value 1-3> | query_interval <sec 1-31744>| max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <value 1-25> | state [enable | disable]}
show igmp	{ipif <ipif_name 12>}
show igmp group	{group <group> | ipif <ipif_name 12>}

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

config igmp

Purpose	Used to configure IGMP on the Switch.
Syntax	**config igmp [ipif <ipif_name 12> | all] {version <value 1-3> | query_interval <sec 1-31744> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <value 1-25> | state [enable | disable]}**
Description	This command allows users to configure IGMP on the Switch.
Parameters	*<ipif_name 12>* – The name of the IP interface for which you want to configure IGMP. *all* – Specifies all the IP interfaces on the Switch. *version <value 1-3>* – Select the IGMP version number. *query_interval <sec 1-31744>* – The time in seconds between general query transmissions, in seconds. *max_response_time <sec 1-25>* – Enter the maximum time in seconds that the Switch will wait for reports from members. *robustness_variable <value 1-255>* – This value states the permitted packet loss that guarantees IGMP. *last_member_query_interval <value 1-25>* – The Max Response Time inserted into Group-Specific Queries and Group-and-Source specific queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query and Group-and-Source specific query messages. The default is 1 second *state [enable | disable]* – Enables or disables IGMP for the specified IP interface.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example Usage:

To configure the IGMPv2 for all IP interfaces.

```
DES-3800:admin#config igmp all version 2
Command: config igmp all version 2

Success.

DES-3800:admin#
```

show igmp

Purpose	Used to display the IGMP configuration for the Switch of for a specified IP interface.
Syntax	**show igmp {ipif <ipif_name 12>}**
Description	This command will display the IGMP configuration for the Switch if no IP interface name is specified. If an IP interface name is specified, the command will display the IGMP configuration for that IP interface.
Parameters	*<ipif_name 12>* – The name of the IP interface for which the IGMP configuration will be displayed.
Restrictions	None.

Example usage:

To display IGMP configurations:

```
DES-3800:admin#show igmp
Command: show igmp

IGMP Interface Configurations
QI : Query Interval                   MRT  : Maximum Response Time
RV : Robustness Value                 LMQI : Last Member Query Interval
Interface   IP Address/Netmask   Version   QI    MRT  RV  LMQI State
--------    ------------------   -------   ----  ---  --- ---- --------
System      10.90.90.90/8        1         125   10   2   1    Enabled
p1          20.1.1.1/8           1         125   10   2   1    Enabled

Total Entries: 2

DES-3800:admin#
```

show igmp group

Purpose	Used to display the Switch’s IGMP group table.
Syntax	**show igmp group {group <group> | ipif <ipif_name 12>}**
Description	This command will display the IGMP group configuration.
Parameters	*group <group>* – The ID of the multicast group to be displayed. *<ipif_name 12>* – The name of the IP interface of which the IGMP group is a member.
Restrictions	None.

Example usage:

To display IGMP group table:

```
DES-3800:admin#show igmp group
Command: show igmp group

Interface   Multicast Group  Last Reporter  IP Querier   IP Expire
----------  ---------------  -------------- ------------ ---------
System      224.0.0.2        10.42.73.111   10.48.74.122  260
System      224.0.0.9        10.20.53.1     10.48.74.122  260
System      224.0.1.24       10.18.1.3      10.48.74.122  259
System      224.0.1.41       10.1.43.252    10.48.74.122  259
System      224.0.1.149      10.20.63.11    10.48.74.122  259

Total Entries: 5

DES-3800:admin#
```

28

AUTO CONFIG COMMANDS V3

The auto config function enables the Switch to obtain its configuration from a TFTP server upon booting up.

Command	Parameters
enable autoconfig	
disable autoconfig	
show autoconfig	

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

enable autoconfig

Purpose	Enables the auto-config function and after rebooting, the system will adopt the configuration file from the tftp server.
Syntax	**enable autoconfig**
Description	When this function is enabled, the system ip interface will be changed to DHCP mode immediately. After rebooting the system it will try to get the configuration file from the TFTP server, whose information is configured in the DHCP server. When the system gets the configuration file from the TFTP server, it will apply the configuration to the system. If the system fails to get a configuration file, the Switch will use the local configuration file for booting.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable autoconfig.

```
DES-3800:admin#enable autoconfig
Command: enable autoconfig

Success

DES-3800:admin#
```

disable autoconfig

Purpose	Disables the auto-config function.
Syntax	**disable autoconfig**
Description	When this function is disabled, the Switch will never get the configuration file from the TFTP server even if the current mode is DHCP.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable autoconfig.

```
DES-3800:admin#disable autoconfig
Command: disable autoconfig

Success

DES-3800:admin#
```

show autoconfig

Purpose	Shows the auto-configuration settings.
Syntax	**show autoconfig**
Description	Shows the current auto config setting.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To show the autoconfig settings.

```
DES-3800:admin#show autoconfig
Command: show autoconfig
Autoconfig enabled.

Success

DES-3800:admin#
```

29

DNS RELAY COMMANDS

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

Command	Parameters
config dnsr	[[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>]
enable dnsr	{cache | static}
disable dnsr	{cache | static}
show dnsr	{static}

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

config dnsr

Purpose	Used to configure the DNS relay function.
Syntax	**config dnsr [[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>]**
Description	This command is used to configure the DNS relay function on the Switch.
Parameters	*primary* – Indicates that the IP address below is the address of the primary DNS server. *secondary* – Indicates that the IP address below is the address of the secondary DNS server. *nameserver <ipaddr>* – The IP address of the DNS nameserver. *[add | delete]* – Indicates whether to add or delete the DNS relay function. *<domain_name 32>* – The domain name of the entry. *<ipaddr>* – The IP address of the entry.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To set IP address 10.43.21.12 of primary.

```
DES-3800:admin#config dnsr primary 10.43.21.12
Command: config dnsr primary 10.43.21.12

Success

DES-3800:admin#
```

Example usage:

To add an entry domain name dns1, IP address 10.43.21.12 to DNS static table:

```
DES-3800:admin#config dnsr add static dns1 10.43.21.12
Command: config dnsr add static dns1 10.43.21.12

Success.

DES-3800:admin#
```

Example usage:

To delete an entry domain name dns1, IP address 10.43.21.12 from DNS static table.

```
DES-3800:admin#config dnsr delete static dns1 10.43.21.12
Command: config dnsr delete static dns1 10.43.21.12

Success.

DES-3800:admin#
```

enable dnsr

Purpose	Used to enable DNS relay.
Syntax	**enable dnsr {cache | static}**
Description	This command is used, in combination with the **disable dnsr** command below, to enable and disable DNS Relay on the Switch.
Parameters	*cache* - This parameter will allow the user to enable the cache lookup for the DNS rely on the Switch. *static* - This parameter will allow the user to enable the static table lookup for the DNS rely on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable status of DNS relay:

```
DES-3800:admin#enable dnsr
Command: enable dnsr

Success.

DES-3800:admin#
```

Example usage:

To enable cache lookup for DNS relay.

```
DES-3800:admin#enable dnsr cache
Command: enable dnsr cache

Success.

DES-3800:admin#
```

Example usage:

To enable static table lookup for DNS relay.

```
DES-3800:admin#enable dnsr static
Command: enable dnsr static

Success.

DES-3800:admin#
```

disable dnsr

Purpose	Used to disable DNS relay on the Switch.
Syntax	**disable dnsr {cache | static}**
Description	This command is used, in combination with the **enable dnsr** command above, to enable and disable DNS Relay on the Switch.
Parameters	*cache* – This parameter will allow the user to disable the cache lookup for the DNS relay on the Switch. *static* – This parameter will allow the user to disable the static table lookup for the DNS relay on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable status of DNS relay.

```
DES-3800:admin#disable dnsr
Command: disable dnsr

Success.

DES-3800:admin#
```

Example usage:

To disable cache lookup for DNS relay.

```
DES-3800:admin#disable dnsr cache
Command: disable dnsr cache

Success.

DES-3800:admin#
```

Example usage:

To disable static table lookup for DNS relay.

```
DES-3800:admin#disable dnsr static
Command: disable dnsr static

Success.

DES-3800:admin#
```

show dnsr

Purpose	Used to display the current DNS relay status.
Syntax	**show dnsr {static}**
Description	This command is used to display the current DNS relay status.
Parameters	*static* – Allows the display of only the static entries into the DNS relay table. If this parameter is omitted, the entire DNS relay table will be displayed.
Restrictions	None.

Example usage:

To display DNS relay status:

```
DES-3800:admin#show dnsr
Command: show dnsr


DNSR Status                    : Disabled
Primary Name Server            : 0.0.0.0
Secondary Name Server          : 0.0.0.0
DNSR Cache Status              : Disabled
DNSR Static Cache Table Status : Disabled

DNS Relay Static Table

Domain Name                                 IP Address
-----------------------------------------   ----------------
www.123.com.tw                              10.12.12.123
bbs.ntu.edu.tw                              140.112.1.23

Total Entries: 2

DES-3800:admin#
```

30

DVMRP COMMANDS

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

Command	Parameters
config dvmrp	[ipif <ipif_name 12> | all] {metric <value 1-31> | probe <sec 1-65535> | neighbor_timeout <sec 1-65535> | state [enable | disable]}
enable dvmrp	
disable dvmrp	
show dvmrp neighbor	{ipif <ipif_name 12> | ipaddress <network_address>}
show dvmrp nexthop	{ipaddress <network_address> | ipif <ipif_name 12>}
show dvmrp routing_table	{ipaddress <network_address>}
show dvmrp	{ipif <ipif_name 12>}

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

config dvmrp

Purpose	Used to configure DVMRP on the Switch.
Syntax	**config dvmrp [ipif <ipif_name 12> | all] {metric <value 1-31> | probe <sec 1-65535> | neighbor_timeout <sec 1-65535> | state [enable | disable]}**
Description	This command is used to configure DVMRP on the Switch.
Parameters	*ipif <ipif_name 12>* – The name of the IP interface for which DVMRP is to be configured. *all* – Specifies that DVMRP is to be configured for all IP interfaces on the Switch. *metric <value 1-31>* – Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default is 1. *probe <second 1-65535>* – DVMRP defined an extension to IGMP that allows routers to query other routers to determine if a DVMRP neighbor is present on a given subnetwork or not. This is referred to as a 'probe'. This entry will set an intermittent probe (in seconds) on the device that will transmit dvmrp messages, depending on the time specified. This probe is also used to "keep alive" the connection between DVMRP enabled devices. The default value is 10 seconds. *neighbor_timeout <second 1-65535>* – The time period for which DVMRP will hold Neighbor Router reports before issuing poison route messages. The default value is 35 seconds. *state [enable* | *disable]* – Allows DVMRP to be enabled or disabled.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure DVMRP configurations of IP interface System:

```
DES-3800:admin#config dvmrp ipif System neighbor_timeout 30
metric 1 probe 5
Command: config dvmrp ipif System neighbor_timeout 30 metric 1
probe 5

Success

DES-3800:admin#
```

enable dvmrp

Purpose	Used to enable DVMRP.
Syntax	**enable dvmrp**
Description	This command, in combination with the **disable dvmrp** command below, is used to enable and disable DVMRP on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable DVMRP:

```
DES-3800:admin#enable dvmrp
Command: enable dvmrp

Success.

DES-3800:admin#
```

disable dvmrp

Purpose	Used to disable DVMRP.
Syntax	**disable dvmrp**
Description	This command is used, in combination with the **enable dvmrp** command above, is used to enable and disable DVMRP on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable DVMRP:

```
DES-3800:admin#disable dvmrp
Command: disable dvmrp

Success.

DES-3800:admin#
```

show dvmrp routing_table

Purpose	Used to display the current DVMRP routing table.
Syntax	**show dvmrp routing table [ipaddress <network_address>]**
Description	The command is used to display the current DVMRP routing table.
Parameters	*ipaddress <network_address>* – The IP address and netmask of the destination. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Example usage:

To display DVMRP routing table:

```
DES-3800:admin#show dvmrp routing_table
Command: show dvmrp routing_table

DVMRP Routing Table
Source Address/Netmask  Upstream Neighbor  Metric Learned Interface  Expire
---------------         ---------          ---    -----   ---------  ----
10.0.0.0/8              10.90.90.90        2      Local   System      -
20.0.0.0/8              20.1.1.1           2      Local   ip2         117
30.0.0.0/8              30.1.1.1           2      Dynamic ip3         106

Total Entries: 3

DES-3800:admin#
```

show dvmrp neighbor

Purpose	Used to display the DVMRP neighbor table.
Syntax	**show dvmrp neighbor {ipif <ipif_name 12> | ipaddress <network_address>}**
Description	This command will display the current DVMRP neighbor table.
Parameters	*<ipif_name 12>* – The name of the IP interface for which to display the DVMRP neighbor table. *ipaddress <network_address>* – The IP address and netmask of the destination. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Example usage:

To display DVMRP neighbor table:

```
DES-3800:admin#show dvmrp neighbor
Command: show dvmrp neighbor

DVMRP Neighbor Address Table

Interface    Neighbor Address   Generation ID    Expire Time
----------   -------------      -------------    -------
System       10.2.1.123         2                 35

Total Entries: 1

DES-3800:admin#
```

show dvmrp nexthop

Purpose	Used to display the current DVMRP routing next hop table.
Syntax	**show dvmrp nexthop {ipaddress <network_address> | ipif <ipif_name 12>}**
Description	This command will display the DVMRP routing next hop table.
Parameters	*<ipif_name 12>* – The name of the IP interface for which to display the current DVMRP routing next hop table. *ipaddress <network_address>* – The IP address and netmask of the destination. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Example usage:

To display DVMRP routing next hop table:

```
DES-3800:admin#show dvmrp nexthop
Command: show dvmrp nexthop

Source IP Address/Netmask  Interface Name   Type
-----------------          --------         ---
10.0.0.0/8                 ip2              Leaf
10.0.0.0/8                 ip3              Leaf
20.0.0.0/8                 System           Leaf
20.0.0.0/8                 ip3              Leaf
30.0.0.0/8                 System           Leaf
30.0.0.0/8                 ip2              Leaf

Total Entries: 6

DES-3800:admin#
```

show dvmrp

Purpose	Used to display the current DVMRP settings on the Switch.
Syntax	**show dvmrp {<ipif_name 12>}**
Description	The command will display the current DVMRP routing table.
Parameters	*<ipif_name 12>* – This parameter will allow the user to display DVMRP settings for a specific IP interface.
Restrictions	None.

Example usage:

To show DVMRP configurations:

```
DES-3800:admin#show dvmrp
Command: show dvmrp

DVMRP Global State : Disabled

Interface   IP Address        Neighbor Timeout  Probe  Metric   State
---------   ---------------   ---------------   -----  ------   -------
System     10.90.90.90/8      35                10     1        Disabled
Trinity    12.1.1.1/8         35                10     1        Enabled

Total Entries: 1

DES-3800:admin#
```

31

IP MULTICASTING COMMANDS

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

Command	Parameters
show ipmc cache	{group <group>} {ipaddress <network_address>}
show ipmc	{ipif <ipif_name 12> | protocol [dvmrp | pim]}
show ipfdb	{[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}

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

show ipmc cache

Purpose	Used to display the current IP multicast forwarding cache.
Syntax	**show ipmc cache {group <group>} {ipaddress <network_address>}**
Description	This command will display the current IP multicast forwarding cache.
Parameters	*group <group>* – The multicast group IP address. *ipaddress <network_address>* – The IP address and netmask of the source. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Usage example:

To display the current IP multicast forwarding cache:

```
DES-3800:admin#show ipmc cache
Command: show ipmc cache

Multicast         Source             Upstream     Expire      Routing
Group             Address/Netmask    Neighbor     Time        Protocol
----------------  ----------------   -----------  ------      --------
224.1.1.1         10.48.74.121/32    10.48.75.63  30           dvmrp
224.1.1.1         20.48.74.25 /32    20.48.75.25  20           dvmrp
224.1.2.3         10.48.75.3 /3      10.48.76.6   30           dvmrp

Total Entries: 3

DES-3800:admin#
```

show ipmc

Purpose	Used to display the IP multicast interface table.
Syntax	**show ipmc {ipif <ipif_name 12> | protocol [dvmrp | pim]}**
Description	This command will display the current IP multicast interface table.
Parameters	*<ipif_name 12>* – The name of the IP interface for which to display the IP multicast interface table for. *protocol* – Allows the user to specify whether or not to use one of the available protocols to display the IP multicast interface table. For example, if DVMRP is specified, the table will display only those entries that are related to the DVMRP protocol. • *dvmrp* – Specifying this parameter will display only those entries that are related to the DVMRP protocol. • *pim* - Specifying this parameter will display only those entries that are related to the PIM protocol.
Restrictions	None.

Usage example

To display the current IP multicast interface table by DVMRP entry:

```
DES-3800:admin#show ipmc protocol dvmrp
Command: show ipmc protocol dvmrp

Interface Name    IP Address     Multicast Routing
---------         -----------    -------------
System            10.90.90.90    DVMRP

Total Entries: 1

DES-3800:admin#
```

show ipfdb

Purpose	Used to display the current network address forwarding database.
Syntax	**show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}**
Description	The show ipfdb command displays the current network address forwarding database.
Parameters	*ip_address <ipaddr>* -Displays the specified IP address. *interface <ipif_name 12 >* - Displays the ipfdb in the specified interface. *port <port>* - Displays the ipfdb by the specified port number.
Restrictions	None.

Example usage:

To display network address forwarding table:

```
DES-3800:admin# show ipfdb
Command: show ipfdb

Interface       IP Address         Port     Learned
-------------   ----------------   ------   ----------
System          10.52.41.20        24       Dynamic
v11                11.0.1.5        26       Dynamic
v12                11.0.2.4        27       Dynamic
v30                30.0.0.2        25       Dynamic
v101             100.0.1.100       21       Dynamic
v101             100.0.1.101       21       Dynamic
v102             100.0.2.101       21       Dynamic
v103             100.0.3.100       21       Dynamic
v103             100.0.3.101       21       Dynamic
v104             100.0.4.100       21       Dynamic
v104             100.0.4.101       21       Dynamic
v105             100.0.5.100       21       Dynamic
v105             100.0.5.101       21       Dynamic
v106             100.0.6.100       21       Dynamic
v106             100.0.6.101       21       Dynamic
v107             100.0.7.100       21       Dynamic
v107             100.0.7.101       21       Dynamic
v108             100.0.8.100       21       Dynamic
v108             100.0.8.101       21       Dynamic
v109             100.0.9.100       21       Dynamic

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

32

MD5 COMMANDS

The MD5 configuration commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create md5 key	<key_id 1-255> <password 16>
config md5 key	<key_id 1-255> <password 16>
delete md5 key	<key_id 1-255>
show md5	{key <key_id 1-255>}

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

create md5 key

Purpose	Used to create a new entry in the MD5 key table.
Syntax	**create md5 key <key_id 1-255> <password 16>**
Description	This command is used to create an entry for the MD5 key table.
Parameters	*<key_id 1-255>* – The MD5 key ID. The user may enter a key ranging from 1 to 255. *<password>* – An MD5 password of up to 16 bytes.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example

To create an entry in the MD5 key table:

```
DES-3800:admin# create md5 key 1 dlink
Command: create md5 key 1 dlink

Success.

DES-3800:admin#
```

config md5 key

Purpose	Used to enter configure the password for an MD5 key.
Syntax	**config md5 key <key_id 1-255> <password 16>**
Description	This command is used to configure an MD5 key and password.
Parameters	*<key_id 1-255>* – The previously defined MD5 key ID. *<password 16>* – The user may change the MD5 password for the md5 key. A new password of up to 16 characters can be created.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example

To configure an MD5 Key password:

```
DES-3800:admin#config md5 key 1 taboo
Command: config md5 key 1 taboo
```

```
Success.

DES-3800:admin#
```

delete md5 key

Purpose	Used to delete an entry in the MD5 key table.
Syntax	**delete md5 key <key_id 1-255>**
Description	This command is used to delete a specific entry in the MD5 key table.
Parameters	*<key_id 1-255>* – The MD5 key ID to delete.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example

To delete an entry in the MD5 key table:

```
DES-3800:admin# delete md5 key 1
Command: delete md5 key 1

Success.

DES-3800:admin#
```

show md5

Purpose	Used to display an MD5 key table.
Syntax	**show md5 {key <key_id 1-255>}**
Description	This command will display the current MD5 key table.
Parameters	*<key_id 1-255>* – The MD5 key ID to be displayed.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To display the current MD5 key:

```
DES-3800:admin#show md5
Command: show md5

MD5 Key Table Configurations

Key-ID      Key
------      ----------
1           dlink
2           develop
3           fireball
4           intelligent

Total Entries: 4

DES-3800:admin#
```

33

OSPF CONFIGURATION COMMANDS

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

Command	Parameters
config ospf router_id	<ipaddr>
enable ospf	
disable ospf	
show ospf	
create ospf area	<area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]
delete ospf area	<area_id>
config ospf area	<area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]
show ospf area	{<area_id>}
create ospf host_route	<ipaddr> {area <area_id> | metric <value 1-65535>}
delete ospf host_route	<ipaddr>
config ospf host_route	<ipaddr> {area <area_id> | metric <value 1-65535>}
show ospf host_route	<ipaddr>
create ospf aggregation	<area_id> <network_address> lsdb_type summary {advertise [enable | disable]}
delete ospf aggregation	<area_id> <network_address> lsdb_type summary
config ospf aggregation	<area_id> <network_address> lsdb_type summary {advertise [enable | disable]}
show ospf aggregation	<area_id>
show ospf lsdb	{area <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asextlink]}
show ospf neighbor	<ipaddr>
show ospf virtual_neighbor	{<area_id> <neighbor_id>}
config ospf ipif	[ipif <ipif_name 12> | all] {area <area_id> | priority <value> | hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>] | metric <value 1-65535> | state [enable | disable] | active | passive}
show ospf	{[ipif <ipif_name 12> | all]}
create ospf virtual_link	<area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}
config ospf virtual_link	<area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}
delete ospf virtual_link	<area_id> <neighbor_id>
show ospf virtual_link	<area_id> <neighbor_id>
config ospf default_information_originate	[enable {always [enable | disable] | mettype [1 | 2] | metric <value> | disable]

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

config ospf router_id

Purpose	Used to configure the OSPF router ID.
Syntax	**config ospf router_id <ipaddr>**
Description	This command is used to configure the OSPF router ID.
Parameters	*<ipaddr>* – The IP address of the OSPF router.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure the OSPF router ID:

```
DES-3800:admin#config ospf router_id 10.48.74.122
Command: config ospf router_id 10.48.74.122

Success.

DES-3800:admin#
```

enable ospf

Purpose	Used to enable OSPF on the Switch.
Syntax	**enable ospf**
Description	This command, in combination with the **disable ospf** command below, is used to enable and disable OSPF on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To enable OSPF on the Switch:

```
DES-3800:admin#enable ospf
Command: enable ospf

Success.

DES-3800:admin#
```

disable ospf

Purpose	Used to disable OSPF on the Switch.
Syntax	**disable ospf**
Description	This command, in combination with the **enable ospf** command above, is used to enable and disable OSPF on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To disable OSPF on the Switch:

```
DES-3800:admin#disable ospf
Command: disable ospf

Success.

DES-3800:admin#
```

show ospf

Purpose	Used to display the current OSPF state on the Switch.
Syntax	**show ospf**
Description	This command will display the current state of OSPF on the Switch, divided into the following categories: General OSPF settings OSPF Default Information Originate settings OSPF Interface settings OSPF Area settings OSPF Virtual Interface settings OSPF Area Aggregation settings OSPF Host Route settings
Parameters	None.
Restrictions	None.

Usage example:

To show OSPF state:

```
DES-3800:admin#show ospf
Command: show ospf

OSPF Router ID    : 10.1.1.2
State                       : Enabled

Default Information Originate: Enabled, Not Always
 Metric Type : 1
 Metric Value: 20
OSPF Interface Settings

Interface  IP Address/Netmask Area ID  State    Link     Metric
                                                Status
---------- ------------------ -------- -------  ------   ------
System     10.90.90.90/8      0.0.0.0  Disabled Link DOWN  1
ip2        20.1.1.1/8         0.0.0.0  Disabled Link DOWN  1
ip3        30.1.1.1/8         0.0.0.0  Disabled Link DOWN  1

Total Entries : 3

OSPF Area Settings
Area ID    Type     Stub Import Summary LSA   Stub Default Cost
---------  -----    -----------------------   -----------------
0.0.0.0    Normal   None                      None
10.0.0.0   Normal   None                      None
10.1.1.1   Normal   None                      None
20.1.1.1   Stub     Enabled                   1

Total Entries : 4
```

```
Virtual Interface Configuration

Transit   Virtual          Hello    Dead     Authentication   Link
Area ID   Neighbor Router  Interval Interval                  Status
--------  ---------------  -------- -------- --------------   ------
10.0.0.0  20.0.0.0         10       60       None             DOWN
10.1.1.1  20.1.1.1         10       60       None             DOWN

Total Entries : 2

OSPF Area Aggregation Settings

Area ID          Aggregated          LSDB      Advertise
                 Network Address     Type
---------------  ------------------  --------  ---------

Total Entries : 0

OSPF Host Route Settings

Host Address    Metric   Area ID          TOS
-------------   ------   ---------------  ---

Total Entries : 0

DES-3800:admin#
```

create ospf area

Purpose	Used to configure OSPF area settings.
Syntax	**create ospf area <area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]**
Description	This command is used to create an OSPF area and configure its settings.
Parameters	*<area_id>* – The OSPF area ID. The user may enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *type [normal* | *stub]* – The OSPF area mode of operation – stub or normal. *stub_summary [enable* | *disable]* – Enables or disables the OSPF area to import summary LSA advertisements. *metric <value 0-65535>* – The OSPF area cost between 0 and 65535. 0 denotes that the value will be automatically assigned. The default setting is 0.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To create an OSPF area:

```
DES-3800:admin#create ospf area 10.48.74.122 type
normal
Command: create ospf area 10.48.74.122 type normal


Success.


DES-3800:admin#
```

delete ospf area

Purpose	Used to delete an OSPF area.
Syntax	**delete ospf area <area_id>**
Description	This command is used to delete an OSPF area.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To delete an OSPF area:

```
DES-3800:admin#delete ospf area 10.48.74.122
Command: delete ospf area 10.48.74.122

Success.

DES-3800:admin#
```

config ospf area

Purpose	Used to configure an OSPF area's settings.
Syntax	**config ospf area <area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]**
Description	This command is used to configure an OSPF area's settings.
Parameters	*<area_id>* – The OSPF area ID. The user may enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *type [normal | stub]* – Allows the specification of the OSPF mode of operation – stub or normal. *stub_summary [enable | disable]* – Allows the OSPF area import of LSA advertisements to be enabled or disabled. *metric <value 0-65535>* – The OSPF area stub default cost.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure an OSPF area's settings:

```
DES-3800:admin#config ospf area 10.48.74.122 type stub stub_summary
enable metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary enable
metric 1

Success.

DES-3800:admin#
```

show ospf area

Purpose	Used to display an OSPF area's configuration.
Syntax	**show ospf area {<area_id>}**

show ospf area

Description	This command will display the current OSPF area configuration.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	None.

Usage example:

To display an OSPF area's settings:

```
DES-3800:admin#show ospf area
Command: show ospf area

Area ID       Type    Stub Import Summary LSA  Stub Default Cost
---------     ------  -----------------------  -----------------
0.0.0.0       Normal  None                     None
10.48.74.122 Stub    Enabled                  Enabled

Total Entries: 2

DES-3800:admin#
```

create ospf host_route

Purpose	Used to configure OSPF host route settings.
Syntax	**create ospf host_route <ipaddr> {area <area_id> | metric <value 1-65535>}**
Description	This command is used to configure the OSPF host route settings.
Parameters	*<ipaddr>* – The host's IP address. *<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *metric <value 1-65535>* – A metric between 1 and 65535, which will be advertised.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure the OSPF host route settings:

```
DES-3800:admin#create ospf host_route 10.48.74.122 area
10.1.1.1 metric 2
Command: create ospf host_route 10.48.74.122 area 10.1.1.1
metric 2

Success.

DES-3800:admin#
```

delete ospf host_route

Purpose	Used to delete an OSPF host route.
Syntax	**delete ospf host_route <ipaddr>**
Description	This command is used to delete an OSPF host route.

delete ospf host_route

Parameters	*<ipaddr>* – The IP address of the OSPF host.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To delete an OSPF host route:

```
DES-3800:admin#delete ospf host_route 10.48.74.122
Command: delete ospf host_route 10.48.74.122

Success.

DES-3800:admin#
```

config ospf host_route

Purpose	Used to configure OSPF host route settings.
Syntax	**config ospf host_route <ipaddr> {area <area_id> | metric <value>}**
Description	This command is used to configure an OSPF host route settings.
Parameters	*<ipaddr>* – The IP address of the host. *<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<value>* – A metric between 1 and 65535 that will be advertised for the route.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure an OSPF host route:

```
DES-3800:admin#config ospf host_route 10.48.74.122 area
10.1.1.1 metric 2
Command: config ospf host_route 10.48.74.122 area 10.1.1.1
metric 2

Success.

DES-3800:admin#
```

show ospf host_route

Purpose	Used to display the current OSPF host route table.
Syntax	**show ospf host_route {<ipaddr>}**
Description	This command will display the current OSPF host route table.
Parameters	*<ipaddr>* – The IP address of the host.
Restrictions	None.

Usage example:

To display the current OSPF host route table:

```
DES-3800:admin#show ospf host_route
Command: show ospf host_route
```

```
Host Address    Metric    Area ID       TOS
------------    ------    -----------   ---

Total Entries: 0

DES-3800:admin#
```

create ospf aggregation

Purpose	Used to configure OSPF area aggregation settings.
Syntax	**create ospf aggregation <area_id> <network_address> lsdb_type summary {advertise [enable | disable]}**
Description	This command is used to create an OSPF area aggregation.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<network_address>* – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area. *lsdb_type summary* – The type of address aggregation. *advertise [enable | disable]* – Allows for the advertisement trigger to be enabled or disabled.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To create an OSPF area aggregation:

```
DES-3800:admin#create ospf aggregation 10.1.1.1
10.48.76.122/16 lsdb_type summary advertise enable
Command: create ospf aggregation 10.1.1.1
10.48.76.122/16 lsdb_type summary advertise enable

Success.

DES-3800:admin#
```

delete ospf aggregation

Purpose	Used to delete an OSPF area aggregation configuration.
Syntax	**delete ospf aggregation <area_id> <network_address> lsdb_type summary**
Description	This command is used to delete an OSPF area aggregation configuration.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<network_address>* – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area. *lsdb_type summary* – Specifies the type of address aggregation.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure the OSPF area aggregation settings:

```
DES-3800:admin#delete ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary
Command:  delete ospf aggregation 10.1.1.1 10.48.76..122/16
lsdb_type summary

Success.

DES-3800:admin#
```

config ospf aggregation

Purpose	Used to configure the OSPF area aggregation settings.
Syntax	**config ospf aggregation <area_id> <network_address> lsdb_type summary {advertise [enable | disable]}**
Description	This command is used to configure the OSPF area aggregation settings.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<network_address>* – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area. *lsdb_type summary* – Specifies the type of address aggregation. *advertise [enable | disable]* – Allows for the advertisement trigger to be enabled or disabled.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure the OSPF area aggregation settings:

```
DES-3800:admin#config ospf aggregation 10.1.1.1
10.48.76.122/16 lsdb_type summary advertise enable
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enable

Success.

DES-3800:admin#
```

show ospf aggregation

Purpose	Used to display the current OSPF area aggregation settings.
Syntax	**show ospf aggregation {<area_id>}**
Description	This command will display the current OSPF area aggregation settings.
Parameters	*<area_id>* – Enter this parameter to view this table by a specific OSPF area ID.
Restrictions	None.

Usage example:

To display OSPF area aggregation settings:

```
DES-3800:admin#show ospf aggregation
Command: show ospf aggregation

OSPF Area Aggregation Settings
```

```
Area ID     Aggregated          LSDB          Advertise
            Network Address     Type
---------   -----------------   --------      ---------
10.1.1.1     10.0.0.0/8         Summary       Enabled
10.1.1.1     20.2.0.0/16        Summary       Enabled

Total Entries: 2
```

show ospf lsdb

Purpose	Used to display the OSPF Link State Database (LSDB).
Syntax	**show ospf lsdb {area_id <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asextlink]}**
Description	This command will display the current OSPF Link State Database (LSDB).
Parameters	*area_id <area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *advertise_router <ipaddr>* – The router ID of the advertising router. *type [rtrlink* | *netlink* | *summary* | *assummary* | *asextlink]* – The type of link.
Restrictions	None.

NOTE: When this command displays a "*" (a star symbol) in the OSPF LSDB table for the *area_id* or the *Cost*, this is interpreted as "no area ID" for external LSAs, and as "no cost given" for the advertised link.

Usage example:

To display the link state database of OSPF:

```
DES-3800:admin#show ospf lsdb
Command: show ospf lsdb

Area      LSDB      Advertising   Link State   Cost    Sequence
ID        Type      Router ID     ID                   Number
--------  ----      ------------  -----------  ------  ----------
0.0.0.0   RTRLink   50.48.75.73   50.48.75.73   *      0x80000002
0.0.0.0   Summary   50.48.75.73   10.0.0.0/8    1      0x80000001
1.0.0.0   RTRLink   50.48.75.73   50.48.75.73   *      0x80000001
1.0.0.0   Summary   50.48.75.73   40.0.0.0/8    1      0x80000001
1.0.0.0   Summary   50.48.75.73   50.0.0.0/8    1      0x80000001
*         ASExtLink 50.48.75.73   1.2.0.0/16    20     0x80000001

Total Entries: 5

DES-3800:admin#
```

show ospf neighbor

Purpose	Used to display the current OSPF neighbor router table.
Syntax	**show ospf neighbor {<ipaddr>}**
Description	This command will display the current OSPF neighbor router table.

show ospf neighbor

Parameters	*<ipaddr>* – The IP address of the neighbor router.
Restrictions	None.

Usage example:

To display the current OSPF neighbor router table:

```
DES-3800:admin#show ospf neighbor
Command: show ospf neighbor

IP Address of    Router ID of    Neighbor   Neighbor
Neighbor         Neighbor        Priority   State
--------------   --------------  --------   ------------
10.48.74.122     10.2.2.2        1          Initial

Total Entries: 1

DES-3800:admin#
```

show ospf virtual_neighbor

Purpose	Used to display the current OSPF virtual neighbor router table.
Syntax	**show ospf virtual_neighbor {<area_id> <neighbor id>}**
Description	This command will display the current OSPF virtual neighbor router table.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<neighbor_id>* – The OSPF router ID for the neighbor. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.
Restrictions	None.

Usage example:

To display the current OSPF virtual neighbor table:

```
DES-3800:admin#show ospf virtual_neighbor
Command: show ospf virtual_neighbor

Transit     Router ID of       IP Address of     Virtual Neighbor
Area ID     Virtual Neighbor   Virtual Neighbor  State
-------     -----------        --------------    ----------------
10.1.1.1    10.2.3.4           10.48.74.111      Exchange

Total Entries : 1

DES-3800:admin#
```

config ospf ipif

Purpose	Used to configure the OSPF interface settings.
Syntax	**config ospf [ipif <ipif_name 12> | all] {area <area_id> | priority <value> | hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>] | metric <value 1-65535> | state [enable | disable] | active |**

config ospf ipif

	passive}
Description	This command is used to configure the OSPF interface settings.
Parameters	*<ipif_name 12>* – The name of the IP interface. *all* - All IP interfaces. *area <area_id>* - A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *priority <value>* – The priority used in the election of the Designated Router (DR). A number between 0 and 255. *hello_interval <sec 1-65535>* – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network. *dead_interval <sec 1-65535>* – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval. *metric <value 1-65535 >* – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric. *authentication* – Enter the type of authentication preferred. The user may choose between: • *none* – Choosing this parameter will require no authentication. • *simple <password 8>* – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. • *md5 <key_id 1-255>* – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required. *metric <value 1-65535>* – This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1. *state [enable | disable]* – Used to enable or disable this function. *active | passive* – This parameter is used to assign the designated entry to be an active or passive interface. The default is *active*.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure OSPF interface settings:

```
DES-3800:admin#config ospf ipif System priority 2 hello_interval
15 metric 2 state enable
Command: config ospf ipif System priority 2 hello_interval 15
metric 2 state enable

Success.

DES-3800:admin#
```

show ospf ipif

Purpose	Used to display the current OSPF interface settings for the specified interface name.

show ospf ipif

Syntax	**show ospf ipif {<ipif_name 12>}**
Description	This command will display the current OSPF interface settings for the specified interface name.
Parameters	*<ipif_name 12>* – The IP interface name for which to display the current OSPF interface settings.
Restrictions	None.

Usage Example:

To display the current OSPF interface settings, for a specific OSPF interface:

```
DES-3800:admin#show ospf ipif ipif2
Command: show ospf ipif ipif2

Interface Name:  ipif2            IP Address: 123.234.12.34/24
((Link Up)
Network Medium Type: BROADCAST     Metric:  1
Area ID:  1.0.0.0                  Administrative State:  Enabled
Priority:  1                       DR State:  DR
DR Address:  123.234.12.34         Backup DR Address:  None
Hello Interval:  10                Dead Interval:  40
Transmit Delay:  1                 Retransmit Time:  5
Authentication:  None

Total Entries: 1


DES-3800:admin#
```

show ospf all

Purpose	Used to display the current OSPF settings of all the OSPF interfaces on the Switch.
Syntax	**show ospf all**
Description	This command will display the current OSPF settings for all OSPF interfaces on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To display the current OSPF interface settings, for all OSPF interfaces on the Switch:

```
DES-3800:admin#show ospf all
Command: show ospf all

Interface Name: System           IP Address:  10.42.73.10/8 (Link Up)
Network Medium Type: BROADCAST   Metric:  1
Area ID:  0.0.0.0                Administrative State:  Enabled
Priority:  1                     DR State:  DR
DR Address:  10.42.73.10         Backup DR Address:  None
Hello Interval:  10              Dead Interval:  40
Transmit Delay:  1               Retransmit Time:  5
Authentication:  None

Interface Name:  ipif2           IP Address: 123.234.12.34/24 (Link Up)
Network Medium Type: BROADCAST    Metric:  1
```

```
Area ID:  1.0.0.0                 Administrative State:  Enabled
Priority:  1                      DR State:  DR
DR Address:  123.234.12.34        Backup DR Address:  None
Hello Interval:  10               Dead Interval:  40
Transmit Delay:  1                Retransmit Time:  5
Authentication:  None

Total Entries: 2

DES-3800:admin#
```

create ospf virtual_link

Purpose	Used to create an OSPF virtual interface.
Syntax	**create ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}**
Description	This command is used to create an OSPF virtual interface.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<neighbor_id>* – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router. *hello_interval <sec 1-65535>* – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network. *dead_interval <sec 1-65535>* – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval. *authentication* – Enter the type of authentication preferred. The user may choose between: • *none* – Choosing this parameter will require no authentication. • *simple <password 8>* – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. • *md5 <key_id 1-255>* – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To create an OSPF virtual interface:

```
DES-3800:admin#create ospf virtual_link 10.1.12 20.1.1.1
hello_interval 10
Command: create ospf virtual_link 10.1.12 20.1.1.1
hello_interval 10


Success.
```

```
DES-3800:admin#
```

config ospf virtual_link

Purpose

Used to configure the OSPF virtual interface settings.

Syntax

config ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}

Description

This command is used to configure the OSPF virtual interface settings.

Parameters

<area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

<neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.

hello_interval <sec 1-65535> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.

dead_interval <sec 1-65535> – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.

authentication – Enter the type of authentication preferred. The user may choose between:

- *none* – Choosing this parameter will require no authentication.
- *simple <password 8>* – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters.
- *md5 <key_id 1-255>* – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.

Restrictions

Only Administrator-level users can issue this command.

Usage example:

To configure the OSPF virtual interface settings:

```
DES-3800:admin#config ospf virtual_link 10.1.1.2 20.1.1.1
hello_interval 10
Command: config ospf virtual_link 10.1.1.2 20.1.1.1
hello_interval 10

Success.

DES-3800:admin#
```

delete ospf virtual_link

Purpose	Used to delete an OSPF virtual interface.
Syntax	**delete ospf virtual_link <area_id> <neighbor_id>**
Description	This command will delete an OSPF virtual interface from the Switch.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<neighbor_id>* – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To delete an OSPF virtual interface from the Switch:

```
DES-3800:admin#delete ospf virtual_link 10.1.12
20.1.1.1
Command: delete ospf virtual_link 10.1.12
20.1.1.1

Success.

DES-3800:admin#
```

show ospf virtual_link

Purpose	Used to display the current OSPF virtual interface configuration.
Syntax	**show ospf virtual_link {<area_id> <neighbor_id>}**
Description	This command will display the current OSPF virtual interface configuration.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<neighbor_id>* – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To display the current OSPF virtual interface configuration:

```
DES-3800:admin#show ospf virtual_link
Command: show ospf virtual_link

Virtual Interface Configuration

Transit   Virtual         Hello     Dead      Authentication  Link
Area ID   Neighbor Router Interval  Interval                 Status
--------- --------------- --------  --------  -------------- ------
10.0.0.0  20.0.0.0        10        60        None            DOWN
```

```
Total Entries: 1

DES-3800:admin#
```

config ospf default_information_originate

Purpose	Used to configure the advertising of a default route into OSPF on the Switch.
Syntax	**config ospf default_information_originate [enable {always [enable | disable] | mettype [1 | 2] metric <value>} | disable]**
Description	This command configures the advertising of a default route into OSPF on the Switch.
Parameters	*enable* – Allows the generation and advertisement of a default route into OSPF. *disable* – Disallows the generation and advertisement of a default route into OSPF. *always* – *enable*- If the advertising router already has a default route, advertise it into OSPF. Otherwise, generate a default route and advertise it into OSPF. *disable*- The default route will only be advertised when the default route exists in the redistributed routes. mettype- Specifies the type of AS external route. metric- Specifies the cost of the default route to be advertised into OSPF. The range is from 0 to 16777214. The metric value 0 will be set in OSPT as the metric value 20.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure OSPF default information originate:

```
DES-3800:admin#config ospf default_information_originate
enable always enable mettype 1 metric 20
Command: config ospf default_information_originate enable
always enable mettype 1 metric 20

Success.

DES-3800:admin#
```

34

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 the SNTP information will be taken from. • *<ipaddr>* – The IP address of the primary server. *secondary* – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable. • *<ipaddr>* – The IP address for the secondary server. *poll-interval <int 30-99999>* – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.
Restrictions	Only Administrator or Operator-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-3800:admin#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-3800:admin#
```

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-3800:admin#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-3800:admin#
```

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 or Operator-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-3800:admin#enable sntp
Command: enable sntp

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example:

To disable SNTP support:

```
DES-3800:admin#disable sntp
Command: disable sntp

Success.

DES-3800:admin#
```

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 or Operator-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-3800:admin#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DES-3800:admin#config time_zone operator + hour 2 min
30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3800:admin#
```

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.

config dst	
Parameters	*disable* - Disable the DST seasonal time adjustment for the Switch. *repeating* - Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October. *annual* - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. *s_week* - Configure the week of the month in which DST begins. *<start_week 1-4,last>* - The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *e_week* - Configure the week of the month in which DST ends. • *<end_week 1-4,last>* - The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *s_day* – Configure the day of the week in which DST begins. • *<start_day sun-sat>* - The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *e_day* - Configure the day of the week in which DST ends. • *<end_day sun-sat>* - The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *s_mth* - Configure the month in which DST begins. • *<start_mth 1-12>* - The month to begin DST expressed as a number. *e_mth* - Configure the month in which DST ends. • *<end_mth 1-12>* - The month to end DST expressed as a number. *s_time* – Configure the time of day to begin DST. • *<start_time hh:mm>* - Time is expressed using a 24-hour clock, in hours and minutes. *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 or Operator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DES-3800:admin#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-3800:admin#
```

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-3800:admin#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-3800:admin#
```

35

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 0-16> | 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 0-16> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the *<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 0-16>* - Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports. *lock_address_mode [Permanent* | *DeleteOnTimout* | *DeleteOnReset]* – Indicates the method of locking addresses. The user has three choices: ▪ *Permanent* – The locked addresses will not age out 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 or Operator-level users can issue this command.

Example usage:

To configure the port security:

```
DES-3800:admin#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-3800:admin#
```

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 which the user wishes to delete. *mac_address <macaddr>* - Enter the corresponding MAC address, previously learned by the port, which the user wishes to delete. *port <port>* - Enter the port number which has learned the previously entered MAC address.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete a port security entry:

```
DES-3800:admin#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-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To clear a port security entry by port:

```
DES-3800:admin# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DES-3800:admin#
```

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-3800:admin#show port_security ports 1-5
Command: show port_security ports 1-5

Port   Admin State    Max. Learning Addr.   Lock Address Mode
----   -----------    -------------------   -----------------
1      Disabled       1                     DeleteOnReset
2      Disabled       1                     DeleteOnReset
3      Disabled       1                     DeleteOnReset
4      Disabled       1                     DeleteOnReset
5      Disabled       1                     DeleteOnReset

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

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	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the port security trap log setting:

```
DES-3800:admin##enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-3800:admin#
```

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	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the port security trap log setting:

```
DES-3800:admin#enable port_security
trap_log
Command: enable port_security trap_log

Success.

DES-3800:admin#
```

36

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 or Operator-level users can issue this command.

Example usage:

To enable MAC notification without changing basic configuration:

```
DES-3800:admin#enable mac_notification
Command: enable mac_notification

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To disable MAC notification without changing basic configuration:

```
DES-3800:admin#disable mac_notification
Command: disable mac_notification

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#config mac_notification interval 1
historysize 500
Command: config mac_notification interval 1 historysize
500

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DES-3800:admin#config mac_notification ports 7
enable
Command: config mac_notification ports 7 enable

Success.
```

```
DES-3800:admin#
```

show mac_notification

Purpose	Used to display the Switch’s MAC address table notification global settings
Syntax	**show mac_notification**
Description	This command is used to display the Switch’s MAC address table notification global settings.
Parameters	None.
Restrictions	None.

Example usage:

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

```
DES-3800:admin#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State         : Enabled
Interval      : 1
History Size  : 1

DES-3800:admin#
```

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-3800:admin#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
```

37

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:

1. 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.
2. 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 user authmode command. There are three choices as to the method SSH will use to authorize the user, and they are password, publickey and hostbased.
3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH Client and the SSH Server.
4. Finally, enable SSH on the Switch using the **enable ssh** command.

After following the above steps, you 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 ssh	
Purpose	Used to enable SSH.
Syntax	**enable ssh**
Description	This command allows you to enable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To enable SSH:

```
DES-3800:admin#enable ssh
Command: enable ssh

Success.

DES-3800:admin#
```

disable ssh

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

Usage example:

To disable SSH:

```
DES-3800:admin# disable ssh
Command: disable ssh

Success.

DES-3800:admin#
```

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 you 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 you to enable or disable SSH authentication on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DES-3800:admin#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

DES-3800:admin#
```

show ssh authmode

Purpose	Used to display the SSH authentication mode setting.
Syntax	**show ssh authmode**
Description	This command will allow you 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-3800:admin#show ssh authmode
Command: show ssh authmode

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

DES-3800:admin#
```

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 you 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 or Operator-level users can issue this command.

Usage example:

To configure the SSH server:

```
DES-3800:admin# config ssh server maxsession 2 contimeout 300
authfail 2
Command: config ssh server maxsession 2 contimeout 300
authfail 2

Success.

DES-3800:admin#
```

show ssh server

Purpose	Used to display the SSH server setting.
Syntax	**show ssh server**
Description	This command allows you to display the current SSH server setting.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To display the SSH server:

```
DES-3800:admin# 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-3800:admin#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	**config ssh user <username> authmode {hostbased [hostname <domain_name> | hostname_IP <domain_name> <ipaddr>} | password | publickey]**
Description	This command allows configuration of the SSH user authentication method.
Parameters	*<username>* - 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

config ssh user

	user. *password* – This parameter should be chosen if the user wishes to use an administrator defined password for authentication. *publickey* – This parameter should be chosen to use the publickey on a SSH server for authentication.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the SSH user:

```
DES-3800:admin# config ssh user Trinity authmode
Password
Command: config ssh user Trinity authmode Password

Success.

DES-3800:admin#
```

show ssh user

Purpose	Used to display the SSH user setting.
Syntax	**show ssh user**
Description	This command allows you to display the current SSH user setting.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the SSH user:

```
DES-3800:admin#show ssh user
Command: show ssh user

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

DES-3800:admin#
```

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 user 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 you 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 users to enable or disable algorithms entered in this command, on the Switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure SSH algorithm:

```
DES-3800:admin# config ssh algorithm
Blowfish enable
Command: config ssh algorithm Blowfish
enable

Success.

DES-3800:admin#
```

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	Only Administrator or Operator-level users can issue this command.

Usage example:

To display SSH algorithms currently set on the Switch:

```
DES-3800:admin#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm:
3DES           : Enabled
AES128         : Enabled
AES192         : Enabled
AES256         : Enabled
arcfour        : 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-3800:admin#
```

config ssh regenerate hostkey

Purpose	Used to regenerate the host key for the SSH algorithm setting.
Syntax	**config ssh regenerate hostkey**
Description	This command will regenerate the host key for the SSH algorithm setting.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To regenerate the SSH hostkey:

```
DES-3800:admin# config ssh regenerate hostkey
Command: config ssh regenerate hostkey

Success.

DES-3800:admin#
```

38

JUMBO FRAME COMMANDS

Certain switches can support jumbo frames (frames larger than the standard Ethernet frame size of 1536 bytes). To transmit frames of up to 9K (and 9220 bytes tagged), the user can increase the maximum transmission unit (MTU) size from the default of 1536 by enabling the Jumbo Frame command.

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

Command	Parameters
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	

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

enable jumbo_frame

Purpose	Used to enable the jumbo frame function on the Switch.
Syntax	**enable jumbo_frame**
Description	This command will allow ethernet frames larger than 1536 bytes to be processed by the Switch. The maximum size of the jumbo frame may not exceed 9220 bytes.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the jumbo frame function on the Switch:

```
DES-3800:admin#enable jumbo_frame
Command: enable jumbo_frame

Success.

DES-3800:admin#
```

disable jumbo_frame

Purpose	Used to disable the jumbo frame function on the Switch.
Syntax	**disable jumbo_frame**
Description	This command will disable the jumbo frame function on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the jumbo frame function on the Switch:

```
DES-3800:admin#disable jumbo_frame
Command: disable jumbo_frame

Success.

DES-3800:admin#
```

show jumbo_frame

Purpose	Used to show the status of the jumbo frame function on the Switch.
Syntax	**show jumbo_frame**
Description	This command will show the status of the jumbo frame function on the Switch.
Parameters	None.
Restrictions	None.

Usage Example:

To show the jumbo frame status currently configured on the Switch:

```
DES-3800:admin#show jumbo_frame
Command: show jumbo_frame

Off.

DES-3800:admin#
```

39

ACCESS AUTHENTICATION CONTROL COMMANDS

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

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

- TACACS (Terminal Access Controller Access Control System) —Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.

- Extended TACACS (XTACACS) — An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.

- TACACS+ (Terminal Access Controller Access Control System plus) — Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery.

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

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

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

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

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

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

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

Please note that when the user logins to the device successfully through 頁 : 252 TACACS / XTACACS / TACACS+server or none method, the "user" priviledge level is the only level assigned. If the user wants to get the administration privilege level, the user must use the "enable admin" command to promote his privilege level. However when the user logins to the device successfully through the RADIUS server or through the local method, 3 kinds of privilege levels can be assigned to the user and the user can not use the "enable admin" command to promote to the admin privilege level.

If the user has configured the user priviledge attribute of the RADIUS server (example: User A admin level) and the login is successful the device will assign the correct priviledge level (according to the RADIUS server) to the user. However if the user does not configure the user priviledge attribute and logins successfully, the device will assign the "user level" to this user. When assigning the levels *3* is used for the user level, *4* is used for the operator level and *5* is used for the administrator level.

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	

Command	Parameters
config admin local_enable	
config accounting type	[exec | system] state [enable | disable]
show accounting type	

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-3800:admin#enable authen_policy
Command: enable authen_policy

Success.

DES-3800:admin#
```

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-3800:admin#disable authen_policy
Command: disable authen_policy

Success.

DES-3800:admin#
```

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-3800:admin#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DES-3800:admin#
```

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-3800:admin#create authen_login method_list_name
Trinity
Command: create authen_login method_list_name Trinity


Success.


DES-3800:admin#
```

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

config authen_login

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

Parameters

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

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

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

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

config authen_login

	NOTE: Entering *none* or *local* as an authentication protocol will override any other authentication that follows it on a method list or on the default method list.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#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-3800:admin#
```

Example usage:

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

```
DES-3800:admin#config authen_login default method xtacacs
tacacs+ local
Command: config authen_login default method xtacacs tacacs+
local

Success.

DES-3800:admin#
```

delete authen_login method_list_name

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

Example usage:

To delete the method list named “Trinity”:

```
DES-3800:admin#delete authen_login method_list_name
Trinity
Command: delete authen_login method_list_name Trinity

Success.

DES-3800:admin#
```

show authen_login

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

Example usage:

To view the authentication login method list named Trinity:

```
DES-3800:admin#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-3800:admin#
```

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-3800:admin#create authen_enable method_list_name
Permit
Command: show authen_login method_list_name Permit

Success.

DES-3800:admin#
```

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.

config authen_enable	
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 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-3800:admin#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-3800:admin#
```

Example usage:

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

```
DES-3800:admin#config authen_enable default method xtacacs
tacacs+ local
Command: config authen_enable default method xtacacs tacacs+
local

Success.

DES-3800:admin#
```

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-3800:admin#delete authen_enable method_list_name
Permit
Command: delete authen_enable method_list_name Permit

Success.

DES-3800:admin#
```

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* 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-3800:admin#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-3800:admin#
```

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, HTTP) 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-3800:admin#config authen application http login default
Command: config authen application http login default

Success.

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

create authen server_host

Purpose

Used to create an authentication server host.

Syntax

create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit < 1-255>}

Description

This command will create an authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

Parameters

server_host <ipaddr> - The IP address of the remote server host to add.

protocol – The protocol used by the server host. The user may choose one of the following:

- *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol.
- *xtacacs* - Enter this parameter if the server host utilizes the XTACACS protocol.
- *tacacs+* - Enter this parameter if the server host utilizes the TACACS+ protocol.

create authen server_host	
	▪ *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-3800:admin#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-3800:admin#
```

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. *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.

config 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 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-3800:admin#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-3800:admin#
```

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 to delete. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* - Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* - Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* - Enter this parameter if the server host utilizes the

delete authen server_host

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

Example usage:

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

```
DES-3800:admin#delete authen server_host 10.1.1.121
protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol
tacacs+

Success.


DES-3800:admin#
```

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-3800:admin#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
No Use

Total Entries : 1

DES-3800:admin#
```

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-3800:admin#create authen server_group group_1
Command: create authen server_group group_1

Success.

DES-3800:admin#
```

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

config authen server_group

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

Example usage:

To add an authentication host to server group “group_1”:

```
DES-3800:admin# 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-3800:admin#
```

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-3800:admin#delete server_group group_1
Command: delete server_group group_1

Success.

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

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* disables the timeout for the response. 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-3800:admin# config authen parameter
response_timeout 60
Command: config authen parameter response_timeout 60
```

```
Success.

DES-3800:admin#
```

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-3800:admin# config authen parameter
attempt 5
Command: config authen parameter attempt 5

Success.

DES-3800:admin#
```

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-3800:admin#show authen parameter
Command: show authen parameter
```

```
Response timeout : 60 seconds
User attempts    : 5

DES-3800:admin#
```

enable admin

Purpose	Used to promote user level privileges to administrator level privileges
Syntax	**enable admin**
Description	When the user logins to the device successfully through TACACS / XTACACS / TACACS+ server or none method, the "user" privilege level is assigned only. If the user wants to get admin privilege level, the user must use the "enable admin" command to promote his privilege level. But when the user logins to the device successfully through RADIUS server or local method, 3 kinds of privilege level can be assigned to the user and the user can not use the "enable admin" command to promote to admin privilege level. When the Enable Method List is set to TACACS, XTACACS, or RADIUS, the user must create a special account with the username "enable" in order to support the Enable Admin function. This function becomes inoperable when the authentication policy is disabled.
Parameters	None.
Restrictions	Only when user logins the device successfully though TACACS / XTACACS / TACACS+ server or none method can use this command to promote privileges.

Example usage:

To enable administrator privileges on the Switch:

```
DES-3800:admin#enable admin
Password: ******

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

config accounting type

Purpose	Used to configure the accounting feature of the Switch, which will employ a remote RADIUS server to collect information regarding events occurring on the Switch.
Syntax	**config accounting type [exec | system] state [enable | disable]**
Description	This command will employ a remote RADIUS server to collect information regarding events occurring on the Switch. Possible switch events which will trigger the sending of information to the RADIUS server once this feature is enabled are as follows: - Account Session ID - Account Session Time - Account Status Type - Username - Account Terminate Cause - Service Type - Account Authentic - NAS IP Address - Account Delay Time - Calling Station ID - NAS Identifier This command is dependant on the configuration of a RADIUS server, both on the Switch, and remotely, so that the RADIUS server has the proper configurations to both collect and process the information that is being relayed to it by the Switch.
Parameters	*type* – Choose the type of accounting that the Switch will use. The user may choose one of the following two choices. • *exec* – When enabled, the Switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the Switch, using the console, Telnet or SSH. • *system* – When enabled, the Switch will send informational packets to a remote RADIUS server when system events occur on the Switch, such as a system reset or system boot. *state [enable | disable]* – Choose whether to enable or disable the accounting type previously chosen.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the system accounting state:

```
DES-3800:admin#config accounting type system
state enable
Command : config accounting type system state
enable

Success.

DES-3800:admin#
```

show accounting type

Purpose	Used to view the accounting feature's current status on the Switch.
Syntax	**show accounting type**
Description	This command will display the current status of the accounting feature on the Switch. Possible switch events which will trigger the sending of information to the RADIUS server once this feature is enabled are as follows: - Account Session ID - Account Session Time - Account Status Type - Username - Account Terminate Cause - Service Type - Account Authentic - NAS IP Address - Account Delay Time - Calling Station ID - NAS Identifier This feature is dependant on the configuration of a RADIUS server, both on the Switch, and remotely, so that the RADIUS server has the proper configurations to both collect and process the information that is being relayed to it by the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the system accounting state:

```
DES-3800:admin#show accounting type
Command : show accounting type

Accounting State
-----------------------------
Exec      : Disable
System    : Disable

DES-3800:admin#
```

40

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 33 switches (numbered 0-32), including the Commander Switch (numbered 0).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the System 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-3800 Series 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 xStack DES-3800 switch series, 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 Candidate state.
2. CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus the CS cannot directly be converted to a MS.
3. The user can manually configure a CS to become a CaS.
4. A MS can become a CaS by:
   a. Being configured as a CaS through the CS.
   b. If report packets from the CS to the MS time out.
5. The user can manually configure a CaS to become a CS
6. The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional xStack DES-3800 series 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-3800 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 Single IP Management White Paper located on the D-Link website.

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

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

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

enable sim

Purpose	Used to enable Single IP Management (SIM) on the Switch
Syntax	**enable sim**
Description	This command will enable SIM globally on the Switch. SIM features and functions will not function properly unless this function is enabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SIM on the Switch:

```
DES-3800:admin#enable sim
Command: enable sim

Success.

DES-3800:admin#
```

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-3800:admin#disable sim
Command: disable sim

Success.

DES-3800:admin#
```

show sim

Purpose	Used to view the current information regarding the SIM group on the Switch.
Syntax	**show sim {[candidates {<candidate_id 1-100>} | members {<member_id 1-32>} | group {commander_mac <macaddr>} | neighbor]}**
Description	This command will display the current information regarding the SIM group on the Switch, including the following: SIM Version - Displays the current Single IP Management version on the Switch. Firmware Version - Displays the current Firmware version on the

show sim	
	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 1-100>* - Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's ID number, listed from 1 to 100. *members <member_id 1-32>* - Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's id number, listed from 1 to 32. *group {commander_mac <macaddr>}* - Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group. *neighbor* – Entering this parameter will display neighboring devices of the Switch. A SIM neighbor is defined as a switch that is physically connected to the Switch but is not part of the SIM group. This screen will produce the following results: • Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located. • MAC Address – Displays the MAC Address of the neighbor switch. • Role – Displays the role(CS, CaS, MS) of the neighbor switch.
Restrictions	None.

Example usage:

To show the SIM information in detail:

```
DES-3800:admin#show sim
Command: show sim

Group Name         : default
SIM Version        : VER-1.61
Firmware Version   : 3.00.B15
Device Name        :
MAC Address        : 00-10-20-33-45-00
Capabilities       : L3
Platform           : DES-3828 L3 Switch
SIM State          : Disabled
Role State         : Candidate
Discovery Interval : 30 sec
Holdtime           : 100 sec
```

```
DES-3800:admin#
```

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

```
DES-3800:admin#show sim candidates 2
Command: show sim candidates 2

ID   MAC Address        Platform /          Hold  Firmware  Device Name
                        Capability          Time  Version
---  -----------------  -------------       ----- -------   ------------
2    00-55-55-00-55-00  DES-3828 L3 Switch  140   3.00-B15  default master

Total Entries: 2

DES-3800:admin#
```

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

```
DES-3800:admin#show sim member 1
Command: show sim member 1

ID   MAC Address        Platform /          Hold  Firmware  Device Name
                        Capability          Time  Version
---  -----------------  -------------       ----- -------   ------------
1    00-01-02-03-04-00  DES-3828 L3 Switch  40    3.00-B15  The Man

Total Entries: 2

DES-3800:admin#
```

To show other groups information in summary:

```
DES-3800:admin#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-3828 L3 Switch  40    3.00-B15  Trinity
 2  00-55-55-00-55-00   DES-3828 L3 Switch  140   3.00-B15  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-3828 L3 Switch  40    3.00-B15  Neo
 2  00-55-55-00-55-00   DES-3828 L3 Switch  140   3.00-B15  default master

‘*’ means commander switch.

DES-3800:admin#
```

Example usage:

To view SIM neighbors:

```
DES-3800:admin#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-3800:admin#
```

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 the user desires 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-3800:admin#reconfig  member_id 2
Command: reconfig  member_id 2

DES-3800:admin#
Login:
```

config sim_group

Purpose	Used to add candidates and delete members from the SIM group.
Syntax	**config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]**
Description	This command is used to add candidates and delete members from the SIM group by ID number.
Parameters	*add <candidate_id 1-100> <password>* - Use this parameter to change a candidate switch (CaS) to a member switch (MS) of a SIM group. The CaS may be defined by its ID number and a password (if necessary). *delete <member_id 1-32>* - Use this parameter to delete a member switch of a SIM group. The member switch should be defined by ID number.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a member:

```
DES-3800:admin#config sim_group add 2
Command: config sim_group add 2

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

Success.

DES-3800:admin#
```

To delete a member:

```
DES-3800:admin#config sim_group delete 1
Command: config sim_group delete 1

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

Success.

DES-3800:admin#
```

config sim	
Purpose	Used to configure role parameters for the SIM protocol on the Switch.
Syntax	**config sim [[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>]**
Description	This command is used to configure parameters of switches of the SIM.
Parameters	*commander* – Use this parameter to configure the commander switch(CS) for the following parameters: ▪ *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 100-255>* – 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 255 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

config sim	
	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.

To change the time interval of the discovery protocol:

```
DES-3800:admin# config sim commander
dp_interval 40
Command: config sim commander dp_interval 40

Success.

DES-3800:admin#
```

To change the hold time of the discovery protocol:

```
DES-3800:admin# config sim hold_time 120
Command: config sim hold_time 120

Success.

DES-3800:admin#
```

To transfer the CS (commander) to be a CaS (candidate):

```
DES-3800:admin# config sim candidate
Command: config sim candidate

Success.

DES-3800:admin#
```

To transfer the Switch to be a CS:

```
DES-3800:admin# config sim commander
Command: config sim commander

Success.

DES-3800:admin#
```

To update the name of a group:

```
DES-3800:admin# config sim commander group_name Trinity
Command: config sim commander group_name Trinity

Success.

DES-3800:admin#
```

download sim_ms	
Purpose	Used to download firmware or configuration file to an indicated device.
Syntax	**download sim [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}**
Description	This command will download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	*firmware_from_tftp* – Specify this parameter to download firmware to members of a SIM group. *configuration_from_tftp* - Specify this parameter to download a switch configuration to members of a SIM group. *<ipaddr>* – Enter the IP address of the TFTP server. *<path_filename>* – Enter the path and the filename of the firmware or switch on the TFTP server. *members* – Enter this parameter to specify the members the user prefers to download firmware or switch configuration files to. The user may specify a member or members by adding one of the following: ▪ *<mslist 1-32>* - Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration. ▪ *all* – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download firmware:

```
DES-3800:admin# download sim_ms firmware_from_tftp 10.53.13.94
c:/des3828.had all
Command: download sim_ms firmware_from_tftp 10.53.13.94
c:/des3828.had 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-3800:admin#
```

To download configuration files:

```
DES-3800:admin# download sim configuration_from_tftp 10.53.13.94
c:/des3828.txt all
Command: download sim configuration_from_tftp 10.53.13.94
c:/des3828.txt 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-3800:admin#
```

upload sim_ms

Purpose	User to upload a configuration file to a TFTP server from a specified member of a SIM group.
Syntax	**upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> {[members <mslist> | all]}**
Description	This command will upload a configuration file to a TFTP server from a specified member of a SIM group.
Parameters	*configuration_to_tftp* - Specify this parameter if the user wishes to upload a switch configuration to members of a SIM group. *log_to_tftp* - Specify this parameter to download a switch log to members of a SIM group. *<ipaddr>* - Enter the IP address of the TFTP server to upload a configuration file to. *<path_filename>* – Enter a user-defined path and file name on the TFTP server to which to upload configuration files. *members* – Enter this parameter to specify the members the user prefers to upload switch configuration or log files to. 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 switch configuration or log files. ▪ *all* – Add this parameter to specify all members of the SIM group will receive the switch configuration or log files.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DES-3800:admin# 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-3800:admin#
```

41

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 BPDU 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 <1-10> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] |
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] | 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>}
show stp instance_id	{<value 0-4>}

Command	Parameters
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 or Operator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DES-3800:admin#enable stp
Command: enable stp

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DES-3800:admin#disable stp
Command: disable stp

Success.

DES-3800:admin#
```

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

Example usage:

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

```
DES-3800:admin#config stp version mstp
Command: config stp version mstp

Success.

DES-3800:admin#
```

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

config stp

	the designated router in RSTP, 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. 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 <value 1-10>* - The maximum number of BPDU Hello packets transmitted per interval. Default value = 3. *fbpdu [enable | disable]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *enable*.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DES-3800:admin#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

DES-3800:admin#
```

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] | 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. The beginning and end of the port list range are separated by a dash. For example, 1-4 specifies all of the ports between port 1 and port 4. *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 BPDU 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

config stp ports

	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*. *fbpdu [enable* | *disable]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. This function can only be in use when STP is globally disabled and forwarding BPDU packets is enabled. The default is *enabled* and BPDU packets will not be forwarded.
Restrictions	Only Administrator or Operator-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-3800:admin#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-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To create a spanning tree instance 2:

```
DES-3800:admin#create stp instance_id 2
Command: create stp instance_id 2

Success.

DES-3800:admin#
```

config stp instance_id

Purpose	Used to add or delete an STP instance ID.
Syntax	**config stp instance_id <value 1-4> [add_vlan | remove_vlan] <vidlist>**
Description	This command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an *instance_id*. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 16 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time. Note that switches in the same spanning tree region having the same STP *instance_id* must be mapped identically, and have the same configuration *revision_level* number and the same *name*.
Parameters	*<value 1-4>* - Enter a number between 1 and 4 to define the *instance_id*. The Switch supports 16 STP 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*. *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 or Operator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DES-3800:admin#config stp instance_id 2 add_vlan
10
Command : config stp instance_id 2 add_vlan 10

Success.

DES-3800:admin#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DES-3800:admin#config stp instance_id 2
remove_vlan 10
Command : config stp instance_id 2 remove_vlan
10
```

```
Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To delete stp instance ID 2 from the Switch.

```
DES-3800:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DES-3800:admin#
```

config stp priority

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

Example usage:

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

```
DES-3800:admin#config stp priority 4096
instance_id 2
Command : config stp priority 4096 instance_id 2


Success.
```

```
DES-3800:admin#
```

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>}**
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 or Operator-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-3800:admin#config stp mst_config_id revision_level 10
name Trinity
Command: config stp mst_config_id revision_level 10 name
Trinity

Success.

DES-3800:admin#
```

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 port number 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 range of ports to be configured. The beginning and end of the port list range are separated by a dash. For example, 1-4 specifies all of the ports between port 1 and port 4. *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.

config stp mst_ports

	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 or Operator-level users can issue this command.

Example usage:

To designate ports 1 to 2 on, with instance ID 1, to have an auto internalCost and a priority of 0:

```
DES-3800:admin#config stp mst_ports 1-2 instance_id 1 internalCost
auto priority 0
Command: config stp mst_ports 1-2 instance_id 1 internalCost auto
priority 0

Success.

DES-3800:admin#
```

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-3800:admin#show stp
Command: show stp

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

DES-3800:admin#
```

Status 2 : STP enabled for RSTP

```
DES-3800:admin#show stp
Command: show stp

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

DES-3800:admin#
```

Status 3 : STP enabled for MSTP

```
DES-3800:admin#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

DES-3800:admin#
```

show stp ports

Purpose	Used to display the Switch's current *instance_id* configuration.
Syntax	**show stp ports <portlist>**
Description	This command displays the STP Instance Settings and STP Instance Operational Status currently implemented on the Switch.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The beginning and end of the port list range are separated by a dash. For example, 1-4 specifies all of the ports between port 1 and port 4.
Restrictions	None.

Example usage:

To show STP ports 1 through 9:

```
DES-3800:admin#show stp ports 1-9
Command: show stp ports 1-9

MSTP Port Information
 ----------------------
Port Index          : 1    ,   Hello Time: 2 /2     ,     Port STP
enabled
External PathCost   : Auto/200000   ,  Edge Port : No /No ,  P2P : Auto
/Yes
Port Forward BPDU enabled

Msti  Designated Bridge  Internal PathCost Prio  Status        Role
----  -----------------  ----------------- ----  -------       ------
0      8000/0050BA7120D6  200000           128   Forwarding    Root
1      8001/0053131A3324  00000            128   Forwarding    Master
```

```
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-3800:admin#show stp instance_id 0
Command: show stp instance_id 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-3800:admin#show stp mst_config_id
Command: show stp mst_config_id
```

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

Configuration Name : [00:10:20:33:45:00               ]
Revision Level :0
MSTI ID     Vid list
-------     -----------
   CIST     1-4094

DES-3800:admin#
```

42

SSL COMMANDS

Secure Sockets Layer or *SSL* is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a *ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the cyphersuite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE_DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES_EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

3. **Hash Algorithm**: This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

Command	Parameters
enable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
config ssl cachetimeout timeout	<value 60-86400>
show ssl	
show ssl certificate	
show ssl cachetimeout	
download ssl certificate	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
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 or Operator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DES-3800:admin#enable ssl
Command:enable ssl

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

DES-3800:admin#
```

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 your URL must begin with *https://*. (ex. https://10.90.90.90)

NOTE: When the Web-based Access Control (WAC) feature is enabled on the Switch, SSL cannot be enabled.

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 or Operator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DES-3800:admin#disable ssl
Command: disable ssl

Success.

DES-3800:admin#
```

To disable ciphersuite ***RSA_EXPORT_with_RC4_40_MD5*** only:

```
DES-3800:admin#disable ssl ciphersuite
RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite
RSA_EXPORT_with_RC4_40_MD5

Success.

DES-3800:admin#
```

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.
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	None.

Example usage:

To set the SSL cachetimeout for 7200 seconds:

```
DES-3800:admin#config ssl cachetimeout timeout 7200
Command: config ssl cachetimeout timeout 7200

Success.

DES-3800:admin#
```

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-3800:admin#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DES-3800:admin#
```

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.

show ssl

Parameters	None.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DES-3800:admin#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-3800:admin#
```

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-3800:admin# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DES-3800:admin#
```

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

download certificate_fromTFTP	
	of the certificate file you wish to download. *keyfilename <path_filename 64>* - Enter the path and the filename of the key exchange file you wish to download.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To download a certificate file and key file to the Switch:

```
DES-3800:admin# DES-3800:admin#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-3800:admin#
```

43

VRRP COMMANDS

VRRP or *Virtual Routing Redundancy Protocol* is a function on the Switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master, and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts. Utilizing VRRP, the administrator can achieve a higher available default path cost without needing to configure every end host for dynamic routing or routing discovery protocols.

Statically configured default routes on the LAN are prone to a single point of failure. VRRP is designed to eliminate these failures by setting an election protocol that will assign a responsibility for a virtual router to one of the VRRP routers on the LAN. When a virtual router fails, the election protocol will select a virtual router with the highest priority to be the Master router on the LAN. This retains the link and the connection is kept alive, regardless of the point of failure.

To configure VRRP for virtual routers on the Switch, an IP interface must be present on the system and it must be a part of a VLAN. VRRP IP interfaces may be assigned to every VLAN, and therefore IP interface, on the Switch. VRRP routers within the same VRRP group must be consistent in configuration settings for this protocol to function optimally.

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

Command	Parameters
enable vrrp	{ping}
disable vrrp	{ping}
create vrrp vrid	<vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}
config vrrp vrid	<vrid 1-255> ipif <ipif_name 12> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}
create vrrp ipif	
config vrrp ipif	<ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]]
show vrrp	{ipif <ipif_name 12> {vrid <vrid 1-255>}
delete vrrp	{vrid <vrid 1-255> ipif <ipif_name 12>}

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

enable vrrp

Purpose	To enable the VRRP function on the Switch.
Syntax	**enable vrrp {ping}**
Description	This command will enable the VRRP function on the Switch.
Parameters	*{ping}* – Adding this parameter to the command will allow the virtual IP address to be pinged from other host end nodes to verify connectivity. This will only enable the ping connectivity check function. To enable the VRRP protocol on the Switch, omit this parameter. This command is disabled by default.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable VRRP globally on the Switch:

```
DES-3800:admin#enable vrrp
Command: enable vrrp

Success.

DES-3800:admin#
```

Example usage:

To enable the virtual IP address to be pinged:

```
DES-3800:admin#enable vrrp ping
Command: enable vrrp ping

Success.

DES-3800:admin#
```

disable vrrp

Purpose	To disable the VRRP function on the Switch.
Syntax	**disable vrrp {ping}**
Description	This command will disable the VRRP function on the Switch.
Parameters	*{ping}* - Adding this parameter to the command will stop the virtual IP address from being pinged from other host end nodes to verify connectivity. This will only disable the ping connectivity check function. To disable the VRRP protocol on the Switch, omit this parameter.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable the VRRP function globally on the Switch:

```
DES-3800:admin#disable vrrp
Command: disable vrrp

Success.

DES-3800:admin#
```

Example usage:

To disable the virtual IP address from being pinged:

```
DES-3800:admin#disable vrrp ping
Command: disable vrrp ping

Success.

DES-3800:admin#
```

create vrrp vrid	
Purpose	To create a VRRP router on the Switch.
Syntax	**vrid <vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}**
Description	This command is used to create a VRRP interface on the Switch.
Parameters	*vrid <vrid 1-255>* - Enter a value between 1 and 255 to uniquely identify this VRRP group on the Switch. All routers participating in this group must be assigned the same *vrid* value. This value MUST be different from other VRRP groups set on the Switch. *ipif <ipif_name 12>* - Enter the name of a previously configured IP interface that you wish to create a VRRP entry for. This IP interface must be assigned to a VLAN on the Switch. *ipaddress <ipaddr>* - Enter the IP address that will be assigned to the VRRP router. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group. *state [enable* | *disable]* - Used to enable and disable the VRRP router on the Switch. *priority <int 1-254>* - Enter a value between 1 and 254 to indicate the router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100. (The value of 255 is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.) *advertisement_interval <int 1-255>* - Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all routers participating within the same VRRP group. The default is 1 second. *preempt [true* | *false]* - This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A true entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A false entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is true. *critical_ip <ipaddr>* - Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will be disabled automatically. A new master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections. *critical_ip_state [enable* | *disable]* - This parameter is used to enable or disable the critical IP address entered above. The default is disable.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create a VRRP entry:

```
DES-3800:admin#create vrrp vrid 1 ipif Darren ipaddress
11.1.1.1 state enable priority 200 advertisement_interval
1 preempt true critical_ip 10.53.13.224 critical_ip_state
enable
Command: create vrrp vrid 1 ipif Darren ipaddress 11.1.1.1
state enable priority 200 advertisement_interval 1 preempt
true critical_ip 10.53.13.224 critical_ip_state enable


Success.


DES-3800:admin#
```

config vrrp vrid

Purpose	To configure a VRRP router set on the Switch.
Syntax	**config vrrp vrid <vrid 1-255> ipif <ipif_name 12> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}**
Description	This command is used to configure a previously created VRRP interface on the Switch.
Parameters	*vrid <vrid 1-255>* - Enter a value between 1 and 255 that uniquely identifies the VRRP group to configure. All routers participating in this group must be assigned the same *vrid* value. This value MUST be different from other VRRP groups set on the Switch. *ipif <ipif_name 12>* - Enter the name of a previously configured IP interface to configure a VRRP entry for. This IP interface must be assigned to a VLAN on the Switch. *state [enable* | *disable]* – Used to enable and disable the VRRP router on the Switch. *priority <int 1-254>* - Enter a value between 1 and 254 to indicate the router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100. (The value of 255 is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.) *ipaddress <ipaddr>* - Enter the virtual IP address that will be assigned to the VRRP entry. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group. *advertisement_interval <int 1-255>* - Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all routers participating within the same VRRP group. The default is 1 second. *preempt [true* | *false]* – This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A true entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A false entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is *true*. *critical_ip <ipaddr>* - Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will be disabled automatically. A new master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections. *critical_ip_state [enable* | *disable]* – This parameter is used to enable or disable the critical IP address entered above. The default is *disable*.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure a VRRP entry:

```
DES-3800:admin#config vrrp vrid 1 ipif Trinity state enable priority 100
advertisement_interval 2
Command: config vrrp vrid 1 ipif Trinity state enable priority 100
advertisement_interval 2

Success.

DES-3800:admin#
```

create vrrp ipif	
Purpose	Creates a virtual router on an interface.
Syntax	**create vrrp ipif <ipif_name 12> vrid <vrid 1-255> ipaddress <ipaddr> {state [enable|disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true|false] | critical_ip <ipaddr> | critical_ip_state [enable|disable]}**
Description	Use this command to create a virtual route on an interface.
Parameters	*ipif*- Specify the name of interface *vrid*- Specify the ID of Virtual Router *Ipaddress*- The virtual router's IP address *state*- Enable/disable the virtual router function *priority*- Specify the priority to be used for the Virtual Router master election process *advertisement_interval*- The time interval, in seconds, between sending advertisement messages *preempt*- Controls whether a higher priority virtual router will preempt a lower priority master *critical_ip*- Specify an IP address of a critical interface *critical_ip_state*- Enable/disable checking the status(active or inactive) of critical ip
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create VRRP:

```
DES-3800:admin #create vrrp ipif System vrid 2 ipaddress
10.1.1.1 state enable
Command: create vrrp ipif System vrid 2 ipaddress 10.1.1.1
state enable

Success.

DES-3800:admin#
```

config vrrp ipif	
Purpose	To configure the authentication type for the VRRP routers of an IP interface.
Syntax	**config vrrp ipif <ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]**
Description	This command is used to set the authentication type for the VRRP routers of an IP interface.
Parameters	*ipif <ipif_name 12>* - Enter the name of a previously configured IP interface for which to configure the VRRP entry. This IP interface must be assigned to a VLAN on the Switch. *authtype* – Specifies the type of authentication used. The authtype must be consistent with all routers participating within the VRRP group. The user may choose between: • *none* – Entering this parameter indicates that VRRP protocol exchanges will not be authenticated. • *simple authdata <string 8>* - This parameter, along with an alphanumeric string of no more than eight characters, to set a simple password for comparing VRRP message packets received by a router. If the two passwords are not exactly the same, the packet will be dropped. *ip authdata <string 16>* - This parameter will require the user to set an alphanumeric authentication string of no more than 16 characters to generate a MD5 message digest for authentication in comparing VRRP messages received by the router. If the two values are inconsistent, the packet will be dropped.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To set the authentication type for a VRRP entry:

```
DES-3800:admin#config vrrp ipif Trinity authtype simple
authdata tomato
Command: config vrrp ipif Trinity authtype simple authdata
tomato

Success.

DES-3800:admin#
```

show vrrp

Purpose	To view the VRRP settings set on the Switch.
Syntax	**show vrrp ipif <ipif_name 12> vrid <vrid 1-255>**
Description	This command is used to view current VRRP settings of the VRRP Operations table.
Parameters	*ipif <ipif_name 12>* - Enter the name of a previously configured IP interface for which to view the VRRP settings. This IP interface must be assigned to a VLAN on the Switch. *vrid <vrid 1-255>* - Enter the VRRP ID of a VRRP entry for which to view these settings.
Restrictions	None.

Example usage:

To view the global VRRP settings currently implemented on the Switch (VRRP Enabled):

```
DES-3800:admin#show vrrp
Command: show vrrp

Global VRRP              :Enabled
Non-owner response PING : Disabled

Interface Name          : System
Authentication type     : No Authentication

         VRID                   : 2
         Virtual IP Address     : 10.53.13.3
         Virtual MAC Address    : 00-00-5E-00-01-02
         Virtual Router State   : Master
         State                  : Enabled
         Priority               : 255
         Master IP Address      : 10.53.13.3
         Critical IP Address    : 0.0.0.0
         Checking Critical IP   : Disabled
         Advertisement Interval: 1 secs
         Preempt Mode           : True
         Virtual Router Up Time: 2754089 centi-secs
Total Entries :  1

DES-3800:admin#
```

delete vrrp

Purpose	Used to delete a VRRP entry from the switch.
Syntax	**delete vrrp {vrid <vrid 1-255> ipif <ipif_name 12>}**
Description	This command is used to remove a VRRP router running on a local device.
Parameters	*vrid <vrid 1-255>* - Enter the VRRP ID of the virtual router to be deleted. Not entering this parameter will delete all VRRP entries on the Switch. *ipif <ipif_name 12>* - Enter the name of the IP interface which holds the VRRP router to delete.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete a VRRP entry:

```
DES-3800:admin#delete vrrp vrid 2 ipif Trinity
Command: delete vrrp vrid 2 ipif Trinity

Success.

DES-3800:admin#
```

44

SYSTEM SEVERITY

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

Command	Parameters
config system_severity	[trap | log | all] [critical | warning | information]
show system_severity	

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

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 or Operator-level users can issue this command.

Example usage:

To configure the system severity settings for critical traps only:

```
DES-3800:admin#config system_severity trap critical
Command: config system_severity trap critical

Success.

DES-3800:admin#
```

show system_severity

Purpose	To display the current severity settings set on the Switch.
Syntax	**show system_severity**
Description	This command is used to view the severity settings that have been implemented on the Switch using the **config system_severity** command.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To view the system severity settings currently implemented on the Switch:

```
DES-3800:admin#show system_severity
Command: show system_severity

system_severity log     :   information
system_severity trap    :   critical

DES-3800:admin#
```

45

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 or Operator-level users can issue this command.

Example usage:

To config DHCP relay:

```
DES-3800:admin#config dhcp_relay hops 2 time
23
Command: config dhcp_relay hops 2 time 23

Success.

DES-3800:admin#
```

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 which to forward (relay) DHCP/BOOTP relay packets.
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 or Operator-level users can issue this command.

Example usage:

To add an IP destination to the DHCP relay table:

```
DES-3800:admin#config dhcp_relay add ipif System
10.58.44.6
Command: config dhcp_relay add ipif System
10.58.44.6

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To delete an IP destination from the DHCP relay table:

```
DES-3800:admin#config dhcp_relay delete ipif System
10.58.44.6
Command: config dhcp_relay delete ipif System
10.58.44.6

Success.

DES-3800:admin#
```

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. 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, which receives the packet, and 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. The DHCP server will then echo 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 then 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 is connected to the DHCP client that sent the DHCP request.
Parameters	*enable* – Choose this parameter to enable the addition of option 82 information to a packet. *disable*- Choose *disable* the relay agent from inserting and removing 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 or Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DES-3800:admin#config dhcp_relay option_82
state enable
Command: config dhcp_relay option_82 state
enable

Success.

DES-3800:admin#
```

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. 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.
Parameters	*enable* – Choose this parameter to enable validity checking of option 82 within packets.

config dhcp_relay option_82 check

	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 or Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 check:

```
DES-3800:admin#config dhcp_relay option_82 check
enable
Command: config dhcp_relay option_82 check enable

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 policy:

```
DES-3800:admin#config dhcp_relay option_82 policy
replace
Command: config dhcp_relay option_82 policy replace

Success.

DES-3800:admin#
```

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-3800:admin#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-3800:admin#
```

Example usage:

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

```
DES-3800:admin#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-3800:admin#
```

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. If the DHCP server is enabled, DHCP relay can not be enabled. The opposite is also true
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable DHCP relay:

```
DES-3800:admin#enable dhcp_relay
Command: enable dhcp_relay

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

To disable DHCP relay:

```
DES-3800:admin#disable dhcp_relay
Command: disable dhcp_relay

Success.

DES-3800:admin#
```

46

IP-MAC BINDING COMMANDS

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC 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-3800 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 for 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 denoting 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 overlap of some 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 {[strict | loose]} | disable] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] }
show address_binding	[ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]
delete address_binding	[ip-mac [ipaddress <ipaddr> mac_address <macaddr> |all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]
enable address_binding acl_mode	
disable address_binding acl_mode	
enable address_binding trap_log	
disable address_binding trap_log	
show address_binding dhcp_snoop	{[max_entry {ports <portlist> | binding_entry {port <port>}]}
enable address_binding dhcp_snoop	
disable address_binding dhcp_snoop	
clear address_binding dhcp_snoop binding_entry ports	[<portlist> | all]
config address_binding dhcp_snoop max_entry ports	[<portlist> | all] limit [<value 1-10> | no_limit]

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

create address_binding ip_mac ipaddress

Purpose	Used to create an IP-MAC Binding entry.
Syntax	**create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] | 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. If the system is in ARP mode, the arp mode entries and acl mode entries will be effective. If the system is in the acl mode, only the acl mode entries will be active. • *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 or Operator-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DES-3800:admin#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-3800:admin#
```

To create address binding on the Switch for ACL mode:

```
DES-3800:admin#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-3800:admin#
```

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

```
DES-3800:admin#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 **config address_binding ip_mac ipaddress <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. If the system is in ARP mode, the arp mode entries and acl mode entries will be effective. If the system is in the acl mode, only the acl mode entries will be active.
- *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 or Operator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-3800:admin#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-3800:admin#
```

To configure address binding on the Switch for ACL mode:

```
DES-3800:admin#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-3800:admin#
```

config address_binding ip_mac ports	
Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.
Syntax	**config address_binding ip_mac ports [<portlist> | all] { state [enable {[strict | loose]} | disable] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable]}**
Description	This command is used to configure the per port state of IP-MAC binding or configure a state which allows zero IP packets to bypass the switch or configure a state which allows the forwarding of DHCP packets from the switch.
Parameters	*<portlist>* - Specifies a port or range of ports to be configured. *all* – Specifies that all ports on the switch will be configured for address binding. *state* – configure the address binding port state to enable or disable. When the state is enabled, the port will perform the binding check. *strict* - This mode provides a stricter method of control. If the user selects this mode, all packets will be sent to the CPU, thus all packets will not be forwarded by the hardware until the S/W learns the entries for the ports. The port will check ARP packets and IP packets by IP-MAC-PORT Binding entries. When the packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block and other packets will be dropped. The default mode is strict if not specified. The ports with strict mode will capture unicast DHCP packets through the ACL module. If configuring IP-MAC binding port enable in strict mode when IP-MAC binding DHCP_snoop is enabled, it will create an ACL profile and the rules according to the ports. If there are not enough profile or rule space for ACL profile or rule table, it will return a warning message and will not create ACL profile and rules to capture unicast DHCP packets. *loose* - This mode provides a looser way of control. If the user selects loose mode, ARP packets and IP Broadcast packets will be sent to the CPU. The packets will still be forwarded by the hardware until a specific source MAC address is blocked by the software. The port will check ARP packets and IP Broadcast packets by IP-MAC-PORT Binding entries . When the packet is found by the entry, the MAC address will be set to dynamic. If the packet is not found by the entry, the MAC address will be set to block. Other packets will be bypassed. *allow_zeroip* – The configure state which allows zero IP packets to bypass. *forward_dhcppkt* - By default, the DHCP packet with broadcast DA will be flooded. When set to disable, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP snooping is enabled, under this case the DHCP packet which has been trapped by the CPU needs to be forwarded by the software. This setting controls the forwarding behavior in this situation.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure port1 enable address_binding and allow_zeroip state and forward_dhcppkt state:

```
DES-3800:admin# config address_binding ip_mac ports 1 state
enable allow_zeroip enable forward_dhcppkt enable
Command: config address_binding ip_mac ports 1 state enable
allow_zeroip enable forward_dhcppkt enable

Success.

DES-3800:admin#
```

show address_binding

Purpose

Used to display IP-MAC Binding entries.

Syntax

show address_binding [ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]

Description

This command will display IP-MAC 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-3800:admin#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


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-3800:admin#
```

Example usage:

To show blocked address binding:

```
DES-3800:admin#show address_binding blocked
Command: show address_binding blocked

VID   VLAN Name   MAC address        Port  Type
----  ----------- ----------------   ----  -----------
 1     default     00-01-02-03-29-38  7    BlockByAddrBind
 1     default     00-01-02-03-29-39  7    BlockByAddrBind
 1     default     00-01-02-03-29-40  7    BlockByAddrBind

Total entries : 3
DES-3800:admin#
```

delete address_binding

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

Example usage:

To delete an IP-MAC Binding on the Switch:

```
DES-3800:admin#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-3800:admin#
```

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 or Operator-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-3800:admin#enable address_binding
acl_mode
Command: enable address_binding acl_mode

Success.

DES-3800:admin#
```

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 or Operator-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-3800:admin#disable address_binding acl_mode
Command: disable address_binding acl_mode

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#enable address_binding
trap_log
Command: enable address_binding trap_log

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#disable address_binding
trap_log
Command: disable address_binding trap_log

Success.

DES-3800:admin#
```

show address_binding dhcp_snoop

Purpose	To show address_binding entries created by DHCP packet.
Syntax	**show address_binding dhcp_snoop {[max_entry {ports <portlist>} | binding_entry {port <port>}]}**
Description	User use this command to show address_binding dhcp_snoop information
Parameters	None.
Restrictions	None.

Example usage:

To show address_binding dhcp_snoop :

```
DES-3800:admin#show address_binding
dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP_Snoop : Enabled

DES-3800:admin#
```

To show address_binding dhcp_snoop binding_entry:

```
DES-3800:admin#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

IP Address     MAC Address        Lease Time   Port Status
-------------  -----------------  -----------  ---- ------
10.1.1.1       00-00-00-00-00-11  1188         1    Active

Total entries : 1

DES-3800:admin#
```

To show address_binding dhcp_snoop max_entry:

```
DES-3800:admin#show address_binding dhcp_snoop
max_entry
Command: show address_binding dhcp_snoop max_entry

Port Max entry
---- ---------
1    5
2    5
3    5
4    5
5    5
6    5
7    5
8    5
9    5
10   5
11   5
12   5
13   5
14   5
15   5
16   5
17   5
18   5
19   5
20   5
21   5
22   5
23   5
24   5
25   5
26   5
27   5
28   5

DES-3800:admin#
```

enable address_binding dhcp_snoop

Purpose	Used to enable address_binding dhcp_snoop
Syntax	**enable address_binding dhcp_snoop**
Description	User uses this command to enable function which entries can be created by DHCP packet.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable address_binding dhcp_snoop:

```
DES-3800:admin#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DES-3800
```

disable address_binding dhcp_snoop

Purpose	Used to disable address_binding dhcp_snoop.
Syntax	disable address_binding dhcp_snoop.
Description	User use this command to disable function which entries can be created by DHCP packet
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable address_binding dhcp_snoop:

```
DES-3800:admin#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DES-3800:admin#
```

clear address_binding dhcp_snoop binding_entry

Purpose	To clear the address binding entries learned for the specified ports.
Syntax	**clear address_binding dhcp_snoop binding_entry ports [<portlist> | all]**
Description	To clear the address binding entries learned for the specified ports.
Parameters	*ports* - Specifies the list of ports that you would like to clear the dhcp-snoop learned entry.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To clear address_binding dhcp_snoop binding_entry:

```
DES-3800:admin#clear address_binding dhcp_snoop
binding_entry ports 1-3
Command: clear address_binding dhcp_snoop
binding_entry ports 1-3

Success.

DES-3800:admin#
```

config address_binding dhcp_snoop max_entry

Purpose	Specifies the max number of entries which can be learned by the specified ports.
Syntax	**config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-10> | no_limit]**
Description	By default, the per port max entry is 5. This command specifies the maximum number of entries which can be learned by the specified ports.
Parameters	*ports* - Specifies the list of ports that you would like to set the maximum dhcp-snoop learned entry. *limit* - Specifies the maximum number.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To set the maximum number of entries that ports can learn:

```
DES-3800:admin#config address_binding dhcp_snoop
max_entry ports 1-3 limit 10
Command: config address_binding dhcp_snoop max_entry
ports 1-3 limit 10

Success.

DES-3800:admin#
```

47

LACP CONFIGURATION COMMANDS

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

Command	Parameters
config lacp_port	<portlist> mode [active | passive]
show lacp_port	{<portlist>}

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

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 or Operator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DES-3800:admin#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DES-3800:admin#
```

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	None.

Example usage:

To display LACP port mode settings:

```
DES-3800:admin#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-3800:admin#
```

48

CPU INTERFACE FILTERING (SOFTWARE ACL) COMMANDS

The xStack DES-3800 switch series implements Access Control Lists that enable the Switch to deny or permit network access to specific devices or device groups based on IP settings, MAC address, and packet content.

Command	Parameters
create cpu access_profile	[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 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 {user_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] [profile_id <value 1-5>]
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> | ethernet_type <hex 0x0-0xffff>} [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>}]} [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>} [permit | deny] | delete access_id <value 1-65535>]
enable cpu interface_filtering	
disable cpu_interface_filtering	
show cpu_interface_filtering	
show cpu access_profile	{profile_id <value 1-5> {access_id <value 1-65535>}}

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> | 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 {user_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] [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 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.
- *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 User Datagram Protocol (UDP) field.
  - *src_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the source port.

create cpu access_profile

	• *dst_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the destination port. • *protocol_id* – Specifies that the switch will examine each frame's Protocol ID field. • *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header. • *packet_content_mask* – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-15* - Enter a value in hex form to mask the packet from byte 0 to byte 15. • *offset_16-31* - Enter a value in hex form to mask the packet from byte 16 to byte 31. • *offset_32-47* - Enter a value in hex form to mask the packet from byte 32 to byte 47. • *offset_48-63* - Enter a value in hex form to mask the packet from byte 48 to byte 63. • *offset_64-79* - Enter a value in hex form to mask the packet from byte 64 to byte 79. *profile_id <value 1-5>* – Specifies an index number that will identify the access profile being created with this command.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To create a CPU access profile:

```
DES-3800:admin#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 1
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 1

Success.

DES-3800:admin#
```

delete cpu access_profile

Purpose	Used to delete a previously created access profile or cpu access profile.
Syntax	**delete cpu access_profile profile_id <value 1-5>**
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 or Operator-level users can issue this command.

Example usage:

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

```
DES-3800:admin#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-3800:admin#
```

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> | ethernet_type <hex 0x0-0xffff>} [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>}]} [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>}[permit | deny] | delete access_id <value 1-65535>]

Description

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

Parameters

profile_id <value 1-5> – 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 cpu 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.

config cpu access_profile	
	• *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 User Datagram Protocol (UDP) field within each packet. • *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this UDP source port in their header. • *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.
	protocol_id <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules. • *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.
	packet_content_mask – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-15* - 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 entry to the CPU or denied entry to the CPU.
	delete access_id <value 1-65535> - Use this to remove a previously created access rule in a profile ID.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure CPU access list entry:

```
DES-3800:admin#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.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example Usage:

To enable CPU interface filtering:

```
DES-3800:admin#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3800:admin#
```

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 or Operator-level users can issue this command.

Example Usage:

To disable CPU filtering:

```
DES-3800:admin#disable cpu_interface_filtering
Command: disable cpu_interface_filtering


Success.

DES-3800:admin#
```

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** state command is used view the current running state of the CPU interface filtering mechanism on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To show the CPU filtering state on the Switch:

```
DES-3800:admin#show cpu_interface_filtering
Command: show cpu_interface_filtering

CPU Interface Filtering : Enabled

DES-3800:admin#
```

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 viewed 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 and 65535 that is used to identify the CPU access profile rule to be viewed with this command. This value is assigned to the access profile rule when it is created with the **config cpu access_profile profile_id** command.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To show the CPU filtering state on the Switch:

```
DES-3800:admin#show cpu access_profile
Command: show cpu access_profile

CPU Access Profile Table

CPU Access Profile ID : 1
Type     : Ethernet
======================================================================
Masks    :
VLAN             802.1p
---------------- ------

CPU Access ID: 1                     Mode: Permit
--------------------------
default
======================================================================

Total Access Entries : 1

DES-3800:admin#
```

49

MODIFY PROMPT AND BANNER COMMANDS

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

Command	Parameters
config command_prompt	[<string 16> | username | default]
config greeting_message	{default}
show greeting_message	

config command_prompt	
Purpose	Used to configure the command prompt for the Command Line Interface.
Syntax	**config command_prompt [<string 16> | username | default]**
Description	This command is used to configure the command prompt for the CLI interface of the Switch. The current command prompt consists of "product name + : + user level + product name" (ex. DES-3800:admin#). The user may replace all parts of the command prompt, except the # by entering a string of 16 alphanumerical characters with no spaces, or the user may enter the current login username configured on the Switch.
Parameters	<*string 16*> - Enter an alphanumeric string of no more than 16 characters to define the command prompt for the CLI interface. *username* – Entering this parameter will replace the current CLI command prompt with the login username configured on the Switch. *default* – Entering this parameter will return the command prompt to its original factory default setting.
Restrictions	The **reset** command will not alter the configured command prompt, yet the **reset system** command will return the command prompt to its original factory default setting. Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the command prompt:

```
DES-3800:admin#config command prompt Trinity
Command: config command prompt Trinity

Success.

 DES-3800:admin#
```

config greeting_message

Purpose	Used to configure the greeting message or banner for the opening screen of the Command Line Interface.
Syntax	**config greeting_message {default}**
Description	This command is used to configure the greeting message or login banner for the opening screen of the CLI.
Parameters	*default* – Adding this parameter will return the greeting command to its original factory default configuration.
Restrictions	The **reset** command will not alter the configured greeting message, yet the **reset system** command will return the greeting message to its original factory default setting. The maximum character capacity for the greeting banned is 6 lines and 80 characters per line. Entering Ctrl+W will save the current configured banner to the DRAM only. To enter it into the FLASH memory, the user must enter the save command. Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the greeting message:

```
DES-3800:admin#config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================
              DES-3828 Fast Ethernet Switch Command Line Interface

                            Firmware: Build 4.50.B10
        Copyright(C) 2000-2005 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
--------------------------------------------------------------------------------

Success.

DES-3800:admin#
```

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-3800:admin#show greeting_message
Command: show greeting_message

=========================================================================
           DES-3828 Fast Ethernet Switch Command Line Interface

                         Firmware: Build 4.50.B10
     Copyright(C) 2000-2005 D-Link Corporation. All rights reserved.
=========================================================================


DES-3800:admin#
```

50

SAFEGUARD ENGINE

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 only receives a small amount of ARP and IP broadcast packets for a calculated time interval. Every five seconds, the Switch will check to see if there are too many packets flooding the Switch. If the threshold has been crossed, the Switch will initially limit and accept a small amount of ingress ARP and IP broadcast packets for five seconds. After another five-second checking interval arrives, the Switch will again check the ingress flow of packets. If the flooding has stopped, the Switch will again begin accepting all packets. Yet, if the checking shows that there continues to be too many packets flooding the Switch, it will still accept a small amount of ARP and IP broadcast packets for double the time of the previous stop period. This doubling of time for limiting ingress ARP and IP broadcast packets will continue until the maximum time has been reached, which is 320 seconds and every stop from this point until a return to normal ingress flow would be 320 seconds.

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.

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	Used to configure the Safeguard Engine for the Switch.
Syntax	**config safeguard_engine {state [enable | disable] | cpu_utilization {rising_threshold <value 20-100> | falling_threshold <value 20-100>} | trap_log [enable | disable]}**
Description	This command is used to configure the settings for the CPU Safeguard Engine function of this Switch, based on CPU utilization.
Parameters	*state [enable | disable]* – Select the running state of the Safeguard Engine function as enable or disable. *cpu_utilization* – Select this option to trigger the Safeguard Engine function to enable based on the following determinates: • *rising <value 20-100>* - The user can set a percentage value of the rising CPU utilization which will trigger the CPU protection function. Once the CPU utilization rises to this percentage, the Safeguard Engine mechanism will initiate. • *falling <value 20-100>* - The user can set a percentage value of the falling CPU utilization which will trigger the CPU protection 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.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the Switch for CPU protection.

```
DES-3800:admin#config safeguard_engine state enable
cpu_utilization rising 50 falling 30 trap log enable
Command: config safeguard_engine state enable cpu_utilization
rising 50 falling 30 trap log enable

Success.

DES-3800:admin#
```

show safeguard_engine

Purpose	To display the CPU Safeguard Engine parameters currently set in the Switch.
Syntax	**show safeguard_engine**
Description	This command is used to show the CPU Safeguard Engine information currently set on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display current CPU protection parameters:

```
DES-3800:admin#show safeguard_engine
Command: show safeguard_engine

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

DES-3800:admin#
```

51

WRED COMMAND LIST

WRED or Weighted Random Early Discard is another implementation for QoS that will help the overall throughput for your QoS queues. Based on the egress queue of the QoS function set on the Switch, this method will analyze these packets and their QoS queue to determine if there will be an overflow of packets entering the QoS queues and consequentially, minimize the packet flow into these queues by dropping random packets. WRED employs two methods of avoiding congestion within the QoS queue.

1. Every QoS queue has a minimum and a maximum level for acceptance of packets. Once the maximum threshold has been reached for this queue, the Switch will begin discarding all ingress packets, this minimizing the allotted bandwidth for QoS. When below the minimum threshold, the switch will accept all ingress packets.
2. When the ingress packets are somewhere between the maximum and minimum queue, the Switch will use a slope probability function to determine a random method of dropping packets based on the fill percentage of the QoS queue. If queues are closer to being full, the Switch will increase the discarding of random packets to even out the flow to the queues and avoid overflows to higher priority queues.

Command	Parameters
enable wred	
disable wred	
config wred ports	[<portlist> | all] [class_id <class_id 0-7> {drop_start <int 0-100>| drop_slope <int 0-90>} | {drop_start <int 0-100> | drop_slope <int 0-90> | average_time <int 1-32768>}]
show wred	{ports [<portlist> | all]}

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

enable wred

Purpose	Used to enable WRED on the Switch.
Syntax	**enable wred**
Description	This command, along with the **disable wred** command will enable and disable the Weighted Random Early Discard (WRED) mechanism on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable WRED switch wide.

```
DES-3800:admin#enable wred
Command: enable wred

Success.

DES-3800:admin#
```

disable wred

Purpose	Used to disable WRED on the Switch.
Syntax	**disable wred**
Description	This command, along with the **enable wred** command will enable and disable the Weighted Random Early Discard (WRED) mechanism on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable WRED switch wide.

```
DES-3800:admin#disable wred
Command: disable wred

Success.

DES-3800:admin#
```

config wred ports

Purpose	Used to configure the WRED settings on the Switch.
Syntax	**config wred ports [<portlist> | all] [class_id <class_id 0-7> {drop_start <int 0-100> | drop_slope <int 0-90>} | {drop_start <int 0-100> | drop_slope <int 0-90> | average_time <int 1-32768>}]**
Description	This command is used to configure the Weighted Random Early Discard (WRED) parameters on the Switch, on a port by port basis, including the drop start point, drop slope and the average time checking interval.
Parameters	*<portlist>* - Specify a port or group of ports for which to configure WRED settings. A list of ports are configured by entering the first and last port of the list, separated by a dash. Multiple separate ports may be entered by separating them with a comma. *class_id <class_id 0-7>* - Specifies the hardware priority queues to be configured for WRED. If no class ID is chosen, all class IDs will be configured for WRED. *drop start <int 0-100>* - Select a percentage between 0 and 100 to initialize the discarding of random packets. This percentage is based on the fill percentage of the QoS queue stated in the Class ID field. (Once the specified queue reaches the target percentage specified here, the Switch will begin randomly discarding packets). Entering a 0 percentage will drop all incoming packets. *drop_slope <int 0-90>* - Specifies the angle of the drop slope for drop probability of incoming packets. The angle 0 would disable the WRED drop probability for the specified hardware queue. *average_time <int 1-32768>]* - Enter a time, in microseconds, that the Switch will check the CoS queues to determine abnormalities in the settings and boundaries which will trigger the WRED function to initialize. This parameter can only be specified and implemented for ports in the portlist and NOT by individual class.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To config the WRED function parameters for port 2 and class ID 2, with a drop start of 50% and a drop slope of 45º:

```
DES-3800:admin#config wred ports 2 class_id 2 drop_start 50
drop_slope 45
Command: config wred ports 2 class_id 2 drop_start 50
drop_slope 45

Success.

DES-3800:admin#
```

Example usage:

To config the WRED function parameters for port 2 and all class IDs, with a drop start of 50% and a drop slope of 45º and average time of 100 microseconds:

```
DES-3800:admin#config wred ports 2 drop_start 50 drop_slope 45
average_time 100
Command: config wred ports 2 drop_start 50 drop_slope 45
average_time 100

Success.

DES-3800:admin#
```

show wred

Purpose	Used to disable WRED on the Switch.
Syntax	**show wred {ports [<portlist> | all]}**
Description	This command will display the configured parameters for the WRED settings on the Switch.
Parameters	*ports <portlist>* - Specify a port or group of ports for which to display WRED settings. A list of ports are configured by entering the first and last port of the list, separated by a dash. Multiple separate ports may be entered by separating them with a comma. *all* – Specifying this parameter will display the WRED settings for all ports on the Switch.
Restrictions	None.

Example usage:

To display the WRED parameters set on the Switch.

```
DES-3800:admin#show wred ports 1
Command: show wred ports 1

Global WRED : Disabled

Port : 1
Average time : 100 (us)

Class_ID    Drop Start     Drop Slope
--------    ----------     ----------
0           50             45
1           50             45
2           50             45
3           50             45
4           50             45
5           50             45
6           50             45
7           50             45

DES-3800:admin#
```

52

WEB-BASED ACCESS CONTROL (WAC) COMMANDS

Web-based Access Control is another port based access control method implemented similarly to the 802.1x port based access control method previously stated. This function will allow user authentication through a RADIUS server or through the local username and password set on the Switch when a user is trying to access the network via the Switch, if the port connected to the user is enabled for this feature.

The user attempting to gain web access will be prompted for a username and password before being allowed to accept HTTP packets from the Switch. Once accepted, the user will be placed in the configured VLAN that has been set for Web-based Access Control. If denied access, no packets will pass through to the user and thus, will be prompted for a username and password again.

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

Command	Parameters
enable wac	
disable wac	
config wac	{vlan <vlan_name 32> | ports [<portlist> | all] state [enable | disable] | method [local | radius] | default_redirpath <string 128>} logout_timer <min 1-1440>}
create wac user	<username 15> {vlan <vlan_name 32>}
config wac user	<username 15> vlan <vlan_name 32>
delete wac user	<username 15>
show wac user	
show wac	{ports [<portlist> | all]}

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

enable wac

Purpose	Used to enable the Web-based Access Control on the Switch.
Syntax	**enable wac**
Description	This command is used to enable Web-based Access Control globally on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable Web-based Access Control globally on the Switch.

```
DES-3800:admin#enable wac
Command: enable wac

Success.

DES-3800:admin#
```

disable wac

Purpose	Used to disable the Web-based Access Control on the Switch.
Syntax	**disable wac**
Description	This command is used to disable Web-based Access Control globally on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable Web-based Access Control globally on the Switch.

```
DES-3800:admin#disable wac
Command: disable wac

Success.

DES-3800:admin#
```

config wac

Purpose	Used to configure the parameters for the Web-based Access Control feature on this Switch
Syntax	**config wac {vlan <vlan_name 32> | ports [<portlist> | all] state [enable | disable] | method [local | radius] | default_redirpath <string 128>}** logout_timer <min 1-1440>}
Description	This command is used to configure the appropriate switch parameters for the Web-based Access Control, including the specification of a VLAN, ports to be enabled for WAC and the method used to authenticate users trying to access the network via the switch
Parameters	*vlan <vlan_name 32>* **-** Enter the VLAN name which users will be placed when authenticated by the Switch or a RADIUS server. This VLAN should be pre-configured to have limited access rights to web based authenticated users. *ports* – Specify this parameter to add ports to be enabled as Web-based Access Control ports. Only these ports will accept authentication parameters from the user wishing limited access rights through the Switch. • *<portlist>* - Specify a port or range of ports to be set as Web-based Access Control ports. • *all* – Specify this parameter to set all ports as Web-based Access Control ports. *state [enable* |*disable]* – Choose whether to enable or disable the previously set ports and VLAN as Web-based Access Control ports. *method* – Select this parameter to select a method of authentication for users trying to access the network via the switch. There are two options: • *local* – Choose this parameter to use the local authentication method of the Switch as the authenticating method for users trying to access the network via the switch. This is, in fact, the username and password to access the Switch. • *radius* – Choose this parameter to use a remote RADIUS server as the authenticating method for users trying to access the network via the switch. This RADIUS server must have already been pre-assigned by the administrator using the

config wac	
	config radius commands located in the 802.1x section. *default_redirpath* - Enter the URL of the website that authenticated users placed in the VLAN are directed to once authenticated. This path must be entered into this field before the Web-based Access Control can be enabled. *Logout_timer* - Used to determine the autologout timer. If the specific port authenticated, it will be logout automatically after the timer expired.
Restrictions	Only Administrator or Operator-level users can issue this command. The WAC VLAN, ports and method can only be configured separately.

Example usage:

To configure the WAC VLAN:

```
DES-3800:admin#config wac vlan Trinity method local ports
1-5 state enable default_redirpath http://www.dlink.com
Command: config wac vlan Trinity method local ports 1-5
state enable default_redirpath http://www.dlink.com

Success.

DES-3800:admin#
```

Example usage:

To configure the WAC ports:

```
DES-3800:admin#config wac ports 1-7 state enable
Command: config wac ports 1-7 state enable

Success.

DES-3800:admin#
```

Example usage:

To configure the Web-based Access Control method:

```
DES-3800:admin#config wac method local
Command: config wac method local

Success.

DES-3800:admin#
```

NOTE: To enable the Web-based Access Control function, the redirection path field must have the URL of the website that users will be directed to once they enter the limited resource, pre-configured VLAN. Users which attempt Apply settings without the Redirection Page field set will be prompted with an error message and Web-based Access Control will not be enabled. The URL should follow the form http(s)://www.dlink.com

NOTE: The subnet of the IP address of the authentication VLAN must be the same as that of the client, or the client will always be denied authentication.

create wac user

Purpose	Used to create a Web-based Access Control user on the switch
Syntax	**create wac user <username 15> {vlan <vlan_name 32>}**
Description	This command is used to create a Web-based Access Control user on the Switch.
Parameters	*<username 15>* - Enter a username of up to 15 alphanumeric characters used to authenticate users trying to access the network via the Switch. This username must be identical to the one the user enters to access the Web-based Access Control for the Switch. *vlan <vlan_name 32>* - Enter the VLAN name of the VLAN this user will be placed in, once authenticated.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a WAC user on the Switch.

```
DES-3800:admin#create wac user Darren vlan Trinity
Command: create wac user Darren vlan Trinity

Success.

DES-3800:admin#
```

config wac user

Purpose	Used to configure a previously created Web-based Access Control user on the Switch.
Syntax	**config wac user <username 15> vlan <vlan_name 32>**
Description	This command is used to configure a previously created Web-based Access Control user on the Switch.
Parameters	*<username 15>* - Enter a username of up to 15 alphanumeric characters used to authenticate users trying to access the network via the Switch. This username must be identical to the one the user enters to access the Web-based Access Control for the Switch. *vlan <vlan_name 32>* - Enter the VLAN name of the VLAN this user will be placed in, once authenticated, if a change in VLANs is desired.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a WAC user on the Switch.

```
DES-3800:admin#config wac user Peter vlan Trinity
Command: config wac user Peter vlan Trinity

Success.

DES-3800:admin#
```

show wac user

Purpose	Used to display the parameters for a previously created Web-based Access Control user on the Switch.
Syntax	**show wac user**
Description	This command is used to display the parameters for a previously created Web-based Access Control user on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the parameters for the WAC user:

```
DES-3800:admin#show wac user
Command: show wac user

Current Accounts:
Username         VLAN name
---------------  ----------------
Darren           Trinity

Total Entries : 1

DES-3800:admin#
```

show wac

Purpose	Used to display the parameters for the Web-based Access Control settings currently configured on the Switch.
Syntax	**show wac {ports [<portlist> | all]}**
Description	This command is used to display the parameters for the Web-based Access Control settings currently configured on the Switch.
Parameters	*ports <portlist>* - Use this parameter to define ports to be viewed for their Web-based Access Control settings. *all* – Use this parameter to display all ports for their Web-based Access Control settings. Entering no parameters will display the remaining parameters of state, authentication method and Web-based Access Control VLAN currently set on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the WAC parameters

```
DES-3800:admin#show wac
Command: show wac

Web Access Control
-----------------------
State        : Enable
Method       : RADIUS
VLAN         : Trinity
Redir Path   :

DES-3800:admin#
```

Example usage:

To display the WAC enabled ports:

```
DES-3800:admin#show wac ports 1-10
Command: show wac ports 1-10

Port  State  Username IP address  Auth status   Assigned Vlan
----  ------ -------  ----------  -----------   ----------
1     Disable         0.0.0.0       Unauth
2     Disable         0.0.0.0       Unauth
3     Disable         0.0.0.0       Unauth
4     Disable         0.0.0.0       Unauth
5     Disable         0.0.0.0       Unauth
6     Disable         0.0.0.0       Unauth
7     Disable         0.0.0.0       Unauth
8     Disable         0.0.0.0       Unauth
9     Disable         0.0.0.0       Unauth
10    Enable  Darren  0.0.0.0       Unauth        1

DES-3800:admin#
```

NOTE: A successful authentication should direct the client to the stated web page. If the client does not reach this web page, yet does not receive a **Fail!** message, the client will already be authenticated and therefore should refresh the current browser window or attempt to open a different web page.

53

DOUBLE VLAN COMMAND LIST

Along with normal VLAN configurations, this Switch now incorporate Double VLANs. Better known as Q-IN-Q VLANs, Double VLANs allow network providers to expand their VLAN configurations to place VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over complicating configurations on the client's side. Not only will over-complication be avoided, but now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network.

Implementation of this feature adds a VLAN frame to an existing VLAN frame for the ISP VLAN recognition and classification. To ensure devices notice this added VLAN frame, an Ethernet encapsulation, here known as a tpid, is also added to the frame. The device recognizes this tpid and therefore checks the VLAN tagged packet to see if a provider VLAN tag has been added. If so, the packet is then routed through this provider VLAN, which contains smaller VLANs with similar configurations to ensure speedy and guaranteed routing destination of the packet.

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

Command	Parameters
enable double_vlan	
disable double_vlan	
create double_vlan	<vlan_name 32> spvid <vlanid 1-4094> {tpid <hex 0x0-0xffff>}
config double_vlan	<vlan_name> {[add [uplink | access] | delete] <portlist> | tpid <hex 0x0-0xffff>}
delete double_vlan	<vlan_name>
show double_vlan	{<vlan_name>}

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

enable double_vlan

Purpose	Used to enable the Double VLAN feature on the Switch.
Syntax	**enable double_vlan**
Description	This command, along with the **disable double_vlan** command, enables and disables the Double Tag VLAN. When Double VLANs are enabled, the system configurations for VLANs will return to the default setting, in order to enable the Double VLAN mode. In the Double VLAN mode, normal VLANs and GVRP functions are disabled. The Double VLAN default setting is disabled.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the Double VLAN feature on the Switch, thus disabling normal VLANs and GVRP.

```
DES-3800:admin#enable double_vlan
Command: enable double_vlan

Success.

DES-3800:admin#
```

disable double_vlan

Purpose	Used to disable the Double VLAN feature on the Switch.
Syntax	**disable double_vlan**
Description	This command, along with the **enable double_vlan** command, enables and disables the Double Tag VLAN. When Double VLANs are enabled, the system configurations for VLANs will return to the default setting, in order to enable the Double VLAN mode. In the Double VLAN mode, normal VLANs and GVRP functions are disabled. The Double VLAN default setting is disabled.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable the Double VLAN feature on the Switch

```
DES-3800:admin#disable double_vlan
Command: disable double_vlan

Success.

DES-3800:admin#
```

create double_vlan	
Purpose	Used to create a Double VLAN on the Switch.
Syntax	**create double_vlan <vlan_name 32> spvid <vlanid 1-4094> {tpid <hex 0x0-0xffff>}**
Description	This command is used to create a Double VLAN (service provider VLAN) on the Switch.
Parameters	*vlan <vlan_name 32>* - The name of the Double VLAN to be created. The user is to enter an alphanumeric string of up to 32 characters to identify this VLAN. *spvid <vlanid 1-4094>* - The VLAN ID of the service provider VLAN. The user is to identify this VLAN with a number between 1 and 4094. *tpid <hex 0x0-0xffff>-* The tag protocol ID. This ID, identified here in hex form, will help identify packets to devices as Double VLAN tagged packets. The default setting is 0x8100.
Restrictions	Only Administrator or Operator-level users can issue this command. Users must have the Switch enabled for Double VLANs.

```
DES-3800:admin#create double_vlan Trinity spvid 6 tpid
0x9100
Command: create double_vlan Trinity spvid 6 tpid 0x9100

Success.

DES-3800:admin#
```

config double_vlan

Purpose

Used to config the parameters for a previously created Double VLAN on the Switch.

Syntax

config double_vlan <vlan_name> {[add [uplink | access] | delete] <portlist> | tpid <hex 0x0-0xffff>}

Description

This command is used to create a Double VLAN (service provider VLAN) on the Switch.

Parameters

vlan <vlan_name 32> - The name of the Double VLAN to be configured. The user is to enter an alphanumeric string of up to 32 characters to identify this VLAN.

add – Specify this parameter to add ports configured in the *<portlist>* as one of the two following types of ports.

- *uplink* – Add this parameter to configure these ports as uplink ports. Uplink ports are for connecting Switch VLANs to the Provider VLANs on a remote source. Only gigabit ports can be configured as uplink ports.
- *access* - Add this parameter to configure these ports as access ports. Access ports are for connecting Switch VLANs to customer VLANs. Gigabit ports can not be configured as access ports.
- *portlist* – Enter a list of ports to be added to this VLAN. A list of ports are configured by entering the first and last port of the list, separated by a dash. Multiple separate ports may be entered by separating them with a comma.

delete - Specify this parameter to delete ports configured in the *<portlist>* from this VLAN.

- *portlist* – Enter a list of ports to be deleted from this VLAN. A list of ports are configured by entering the first and last port of the list, separated by a dash. Multiple separate ports may be entered by separating them with a comma.

tpid <hex 0x0-0xffff>- The tag protocol ID. This ID, identified here in hex form, will help identify packets to devices as Double VLAN tagged packets. The default setting is 0x8100.

Restrictions

Only Administrator or Operator-level users can issue this command.

Users must have the Switch enabled for Double VLANs.

Example usage:

To add ports 4 through 8 as access ports to the Double VLAN Trinity:

```
DES-3800:admin#config double_vlan Trinity add access 4-
8
Command: config double_vlan Trinity add access 4-8

Success.

DES-3800:admin#
```

Example usage:

To delete ports 4 through 8 on the Double VLAN Trinity:

```
DES-3800:admin#config double_vlan Trinity delete 4-8
Command: config double_vlan Trinity delete 4-8

Success.

DES-3800:admin#
```

show double_vlan

Purpose	Used to display the Double VLAN settings on the Switch.
Syntax	**show double_vlan <vlan_name>**
Description	This command will display the current double VLAN parameters configured on the Switch.
Parameters	*vlan name* - Enter the name of a previously created VLAN for which to display the settings.
Restrictions	None. Users must have the Switch enabled for Double VLANs.

Example usage:

To display parameters for the Double VLAN Trinity:

```
DES-3800:admin#show double_vlan  Trinity
Command: show double_vlan Trinity

Global Double VLAN : Enabled
====================================================
SPVID         : 6
VLAN Name     : Trinity
TPID          : 0x9200
Uplink ports  :
Access ports  : 4-8
Unknow ports  :
----------------------------------------------------
Total Entries : 1

DES-3800:admin#
```

54

LIMITED MULTICAST IP ADDRESS COMMANDS

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

Command	Parameters
create mcast_filter_profile profile_id	<value 1-24> description <desc 1-32>
config mcast_filter_profile profile_id	< value 1-24> { description <desc 1-32> | [add | delete] <mcast_address_list>}
delete mcast_filter_profile profile_id	<value 1-24>
show mcast_filter_profile	{ profile_id <value 1-24>}
config limited_multicast_addr ports	<portlist> { [add | delete] profile_id <value 1-24> | access [permit | deny]}
show limited_multicast_addr	{ ports <portlist>}
config max_mcast_group ports	<portlist> max_group <value 1-256>
show max_mcast_group ports	{ports <portlist>}

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

create mcast_filter_profile

Purpose	This command creates a multicast address profile.
Syntax	**create mcast_filter_profile profile_id <value 1-24> description <desc 1-32>**
Description	This command configures a multicast address profile. Mutliple ranges of multicast addresses can be defined in the profile.
Parameters	*profile_id* - ID of the profile. Range is 1 to24. *description* - Provides a meaningful description for the profile.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To create a multicast filter profile:

```
DES-3800:admin# create mcast_filter_profile profile_id
2 description MOD
Command: create mcast_filter_profile profile_id 2
description MOD


Success.


DES-3800:admin#
```

config mcast_filter_profile

Purpose	This command adds or deletes a range of multicast addresses to the profile.
Syntax	**config mcast_filter_profile profile_id < value 1-24> { profile_name <name> | [add | delete] <mcast_address_list>}**
Description	This command adds or deletes a range of multicast IP addresses previously defined.
Parameters	*profile_id* - ID of the profile. *mcast_address_list* - List of the multicast addresses to be put in the profile. You can either specify a single multicast IP address or a range of multicast addresses using the profile.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To configure a multicast filter profile:

```
DES-3800:admin# config mcast_filter_profile profile_id
2 add 225.1.1.1 - 225.1.1.1
Command: config mcast_filter_profile profile_id 2 add
225.1.1.1 - 225.1.1.1

Success.

DES-3800:admin#
```

delete mcast_filter_profile

Purpose	This command deletes a multicast address profile.
Syntax	**delete mcast_filter_profile profile_id <value 1-24>**
Description	This command deletes a multicast address profile
Parameters	*profile_id* - ID of the profile
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To delete a multicast filter profile:

```
DES-3800:admin# delete mcast_filter_profile profile_id
3
Command: delete mcast_filter_profile profile_id 3

Success.

DES-3800:admin#
```

show mcast_filter_profile

Purpose	This command displays the defined multicast address profiles.
Syntax	**show mcast_filter_profile { profile_id <value 1-24>}**
Description	This command displays the defined multicast address profiles.
Parameters	*profile_id* - ID of the profile. If not specified, all profiles will be displayed.
Restrictions	None.

Usage Example:

To display a multicast filter profile:

```
DES-3800:admin#show mcast_filter_profile
Command: show mcast_filter_profile

Mcast Filter Profile:

Profile_Id:  1
Description: MOD
Mcast Group:
234.1.1.1-235.244.244.244           236.1.1.1-
238.244.244.244

Profile_Id:  1
Description: customer
Mcast Group:
224.19.62.34-224.19.162.200

Total Profile Count : 2

DES-3800:admin#
```

config limited_multicast_addr

Purpose	Used to configure the multicast address filtering function on a port.
Syntax	**config limited_multicast_addr ports <portlist> {[add | delete] profile_id <value 1-24> | access [permit | deny]}**
Description	Used to configure the multicast address filtering function on a port. When there are no profiles specified with a port, the limited function is not effective.
Parameters	*<portlist>* - A range of ports to config the multicast address filtering function. *add* - Add a multicast address profile to a port. *delete* - Delete a multicast address profile to a port. *profile_id* - A profile to be added to or deleted from the port. *permit* - Specifies that the packet that match the addresses defined in the profiles will be permitted. The default mode is permit. *deny* - Specifies that the packet that match the addresses defined in the profiles will be denied.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config port 1,3 to set the multicast address profile 2.

```
DES-3800:admin# config limited_multicast_addr ports
1,3 add profile_id 2
Command: config limited_multicast_addr ports 1,3 add
profile_id 2

Success.

DES-3800:admin#
```

show limited_multicast_addr

Purpose	Used to show per-port Limited IP multicast address range.
Syntax	**show limited_multicast_addr { ports <portlist>}**
Description	The show limited_multicast_addr command allows you to show multicat address range by ports.
Parameters	*<portlist>* - A range of ports to show the limited multicast address configuration.
Restrictions	None.

Usage Example:

To show limited multicast address range:

```
DES-3800:admin#show limited_multicast_addr 1,3
Command: show limited_multicast_addr 1,3


Port    : 1
Access  : Deny
Profile Id: 1

Port    : 3
Access  : Deny
Profile ID: 1

DES-3800:admin#
```

config max_mcast_group

Purpose	This command configures the maximum number of multicast group that a port can join.
Syntax	**config max_mcast_group ports <portlist> max_group <value 1-256>**
Description	This command configures the maximum number of multicast group that a port can join.
Parameters	*<portlist>* - A range of ports to config the max_mcast_group *max_group* - Specifies the maximum number of the multicast groups. The range is from 1 to 256.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To configure the maximum number of multicast groups that a port can join:

```
DES-3800:admin# config max_mcast_group ports 1, 3
max_group 100
Command: config max_mcast_group ports 1, 3 max_group
100

Success.

DES-3800:admin#
```

show max_mcast_group ports

Purpose	This command display the max number of multicast groups that a port can join.
Syntax	**show max_mcast_group ports <portlist>**
Description	This command display the max number of multicast groups that a port can join.
Parameters	*<portlist>* - A range of ports to display the max number of multicast groups.
Restrictions	None.

Usage Example:

To display the maximum number of multicast groups that a port can join:

```
DES-3800:admin# show max_mcast_group ports 1
Command: show max_mcast_group ports 1

Port           Max Multicast Group Number
--------     -----------------------------
100
3     3                    100
DES-3800:admin#
```

55

ROUTE PREFERENCE COMMANDS

Route Preference is a way for routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. The majority of routing protocols are not compatible when used in conjunction with each other. This Switch supports and may be configured for many routing protocols, as a stand alone switch or more importantly, in utilizing the stacking function and Single IP Management of the Switch. Therefore the ability to exchange route information and select the best path is essential to optimal use of the Switch and its capabilities.

The first decision the Switch will make in selecting the best path is to consult the Route Preference Settings table of the Switch. This table can be viewed using the **show route preference** command, and it holds the list of possible routing protocols currently implemented in the Switch, along with a reliability value which determines which routing protocol will be the most dependable to route packets. Below is a list of the default route preferences set on the Switch.

Route Type	Validity Range	Default Value
Local	0 – Permanently set on the Switch and unconfigurable.	0
Static	1 – 999	60
OSPF Intra	1 – 999	80
OSPF Inter	1 – 999	90
RIP	1 – 999	100
OSPF ExtT1	1 – 999	110
OSPF ExtT2	1 – 999	115

As shown above, *Local* will always be the first choice for routing purposes and the next most reliable path is *Static* due to the fact that its has the next lowest value. To set a higher reliability for a route, change its value to a number less than the value of a route preference that has a greater reliability value using the **config route preference** command. For example, if the user wishes to make RIP the most reliable route, the user can change its value to one that is less than the lowest value (Static - 60) or the user could change the other route values to more than 100.

The user should be aware of three points before configuring the route preference.

1. No two route preference values can be the same. Entering the same route preference may cause the Switch to crash due to indecision by the Switch.
2. If the user is not fully aware of all the features and functions of the routing protocols on the Switch, a change in the default route preference value may cause routing loops or black holes.
3. After changing the route preference value for a specific routing protocol, that protocol needs to be restarted because the previously learned routes have been dropped from the Switch. The Switch must learn the routes again before the new settings can take affect.

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

Command	Parameters
config route preference	[static | rip | ospfIntra | ospfInter | ospfExt1 | ospfExt2] <value>
show route preference	{[static | rip | ospfIntra | ospfInter | ospfExt1 | ospfExt2]}

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

config route preference

Purpose

Used to configure the route preference of each route type.

Syntax

config route preference [static | rip | ospfIntra | ospfInter | ospfExt1 | ospfExt2] <value 1-999>

Description

This command is used to set the route preference value for each routing protocol listed. A lower value will denote a better chance that the specified protocol is the best path for routing packets.

Parameters

The user may set a preference value for a specific route by first choosing one of the following and then adding an alternate preference value:

- *static* – Choose this parameter to configure the preference value for the *static* route.
- *rip* - Choose this parameter to configure the preference value for the *RIP* route.
- *ospfIntra* - Choose this parameter to configure the preference value for the *OSPF Intra-area* route.
- *ospfInter* - Choose this parameter to configure the preference value for the *OSPF Inter-area* route.
- *ospfExtT1* - Choose this parameter to configure the preference value for the *OSPF AS External route type-1* route.
- *ospfExtT2* - Choose this parameter to configure the preference value for the *AS External route type-2* route.

<*value 1-999*> - Enter a value between 1 and 999 to set the route preference for a particular route. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets.

Restrictions

Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the route preference value for RIP as 50:

```
DES-3800:admin#config route preference rip 50
Command: config route preference rip 50

Success.

DES-3800:admin#
```

show route preference

Purpose

Used to display the route preference of each route type.

Syntax

show route preference {[static | rip | ospfIntra | ospfInter | ospfExt1 | ospfExt2]}

Description

This command will display the Route Preference Settings table. The user may view all route preference settings by entering the command without any parameters or choose a specific type by adding the route parameter to the command.

Parameters

local – Enter this parameter to view the route preference settings for the *local* route.

static - Enter this parameter to view the route preference settings for the *static* route.

rip - Enter this parameter to view the route preference settings for

show route preference	
	the *RIP* route. *ospfIntra* **-** Enter this parameter to view the route preference settings for the *Ospf Intra-area* route. *ospfInter* - Enter this parameter to view the route preference settings for the *OSPF Inter-area* route. *ospfExtT1* - Enter this parameter to view the route preference settings for the *OSPF AS External route type-1*. *ospfExtT2* - Enter this parameter to view the route preference settings for the *OSPF AS External route type-2.* Entering this command with no parameters will display the route preference for all routes.
Restrictions	None.

Example usage:

To view the route preference values for all routes:

```
DES-3800:admin#show route preference
Command: show route preference

Route Preference Settings

Route Type     Preference
----------     --------
RIP            100
OSPF Intra     80
STATIC         60
LOCAL          0
OSPF Inter     90
OSPF ExtT1     110
OSPF ExtT2     115

DES-3800:admin#
```

Example usage:

To view the route preference values for the RIP route:

```
DES-3800:admin#show route preference rip
Command: show route preference rip

Route Preference Settings

Route Type     Preference
----------     ----------
RIP            100

DES-3800:admin#
```

56

MAC-BASED ACCESS CONTROL COMMANDS

The MAC-Based Access Control feature will allow users to configure a list of MAC addresses, either locally or on a remote RADIUS server, to be authenticated by the Switch and given access rights based on the configurations set on the Switch of the target VLAN where these authenticated users are placed.

The Switch will learn MAC addresses of a device through the receipt of ARP packets or DHCP packets and then attempt to match them on the authenticating list. If the client has not been configured for DHCP or does not have an IP configuration in static mode, then MAC addresses cannot be discovered and the client will not be authenticated. Ports and MAC addresses awaiting authentication are placed in the Guest VLAN where the Switch administrator can assign limited rights and privileges.

For local authentication on the Switch, the user must enter a list of MAC addresses to be accepted through this mechanism using the MAC-Based Access Control Local Database Settings window, as seen below. The user may enter up to 1024 MAC addresses locally on the Switch but only sixteen MAC addresses can be accepted per physical MAC-Based Access Control enabled port. Once a MAC addresses has been authenticated by the Switch on the local side, the port where that MAC address resides will be placed in the previously configured target VLAN, where the rights and privileges are set by the switch administrator. If the VLAN Name for the target VLAN is not found by the Switch, the Switch will return the MAC address to the originating VLAN. If the MAC address is not found, then if the port is in the Guest VLAN, it will remain in the Guest VLAN, with the associated rights. If the port is not in the guest VLAN, this MAC address will be blocked by the Switch.

For remote RADIUS server authentication, the user must first configure the RADIUS server with a list of MAC addresses and relative target VLANs that are to be authenticated on the Switch. Once a MAC address has been discovered by the Switch through ARP or DHCP packets, the Switch will then query the remote RADIUS server with this potential MAC address, using a RADIUS Access Request packet. If a match is made with this MAC address, the RADIUS server will return a notification stating that the MAC address has been accepted and is to be placed in the target VLAN. If the VID for the target VLAN is not found by the Switch, the Switch will create its own MAC-Based Access Control VLAN, named MBA-xx, where the xx is the VID of the first available VLAN ID that can be assigned to this VLAN. If the MAC address is not found, then if the port is in the Guest VLAN, it will remain in the Guest VLAN, with the associated rights. If the port is not in the guest VLAN, this MAC address will be blocked by the Switch.

Notes About MAC-Based Access Control

There are certain limitations and regulations regarding the MAC-Based Access Control:

1. Once this feature is enabled for a port, the Switch will clear the FDB of that port.
2. If a port is granted clearance for a MAC address within a VLAN that is NOT a Guest VLAN, other MAC addresses on that port must be authenticated for access and otherwise will be blocked by the switch.
3. MAC-Based Access Control is its own entity and is not dependant on other authentication functions on the Switch, such as 802.1X, Web-Based authentication etc…
4. For authenticating VLANs that are not Guest VLANs, a port accepts a maximum of sixteen authenticated MAC addresses per physical port. Other MAC addresses attempting authentication on a port with the maximum number of authenticated MAC addresses will be blocked.
5. Ports that have been enabled for Link Aggregation, stacking, 802.1X authentication, 802.1X Guest VLAN, Port Security, GVRP or Web-Based authentication cannot be enabled for the MAC-Based Authentication.

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

Command	Parameters
enable mac_based_access_control	
disable mac_based_access_control	
config mac_based_access_control	{ports [<portlist> | all] state [enable | disable] | method [local | radius] | password <passwd 16>}
show mac_based_access_control	{ports [<portlist> | all]}
create mac_based_access_control guest_vlan	<vlan_name 32>
config mac_based_access_control guest_vlan ports	<portlist>
delete mac_based_access_control guest_vlan	

Command	Parameters
create mac_based_access_control_local mac	<macaddr> vlan <vlan_name 32>
config mac_based_access_control_local mac	<macaddr> vlan <vlan_name 32>
delete mac_based_access_control_local	[mac <macaddr> | vlan <vlan_name 32>]
show mac_based_access_control_local	{[mac <macaddr> | vlan <vlan_name 32]}
show mac_based_access_control auth_mac	{ports <portlist>}

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

enable mac_based_access_control

Purpose	Used to enable the MAC-based Access Control on the Switch.
Syntax	**enable mac_based_access_control**
Description	This command, along with the **disable mac_based_access_control** command is used to enable and disable MAC-based Access Control globally on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable MAC-based Access Control globally on the Switch.

```
DES-3800:admin#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DES-3800:admin#
```

disable mac_based_access_control

Purpose	Used to disable the MAC-based Access Control on the Switch.
Syntax	**disable mac_based_access_control**
Description	This command, along with the **enable mac_based_access_control** command is used to enable and disable MAC-based Access Control globally on the Switch.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To disable MAC-Based Access Control globally on the Switch.

```
DES-3800:admin#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DES-3800:admin#
```

config mac_based_access_control

Purpose

Used to configure the global parameters of the MAC-based Access Control on the Switch.

Syntax

config mac_based_access_control {ports [<portlist> | all] state [enable | disable] | method [local | radius] | password <passwd 16>}

Description

This command is used to configure the global parameters for the MAC-based access control function on the Switch, including enabled ports, method of authentication and the password to be used to access the remote RADIUS server.

Parameters

ports <portlist> - Choose this parameter to configure a list of ports to be enabled for the MAC-based access control function.

state [enable | *disable]* – Use the state parameter to enable or disable the previously set ports as MAC-based access control enabled ports.

method – Use this parameter to choose the type of authentication to be used when authenticating MAC addresses on a given port. The user may choose between the following methods:

- *local* – Use this method to utilize the locally set MAC address database as the authenticator for MAC-Based Access Control. This MAC address list can be configured in the MAC-Based Access Control Local Database Settings window.
- *radius* – Use this method to utilize a remote RADIUS server as the authenticator for MAC-Based Access Control. Remember, the MAC list must be previously set on the RADIUS server and the settings for the server must be first configured on the Switch.

password <passwd 16> - Use this parameter to enter the password of up to 16 alphanumeric characters for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is “default”.

Restrictions

Only Administrator or Operator-level users can issue this command.

Example usage:

To configure MAC-based Access Control global settings on the Switch.

```
DES-3800:admin#config mac_based_access_control ports 1-8 state
enable
Command: config mac_based_access_control ports 1-8 state enable

Success.

DES-3800:admin#
```

show mac_based_access_control	
Purpose	Used to display the global MAC-based Access Control settings on the Switch.
Syntax	**show mac_based_access_control {ports <portlist> | all]}**
Description	This command will display the global settings for the MAC-based access control function on the Switch. Entering this command without the related ports will display the global features for this function. Adding the ports will display the currently set running state of that port for the MAC-based access control function.
Parameters	*ports* – Add this parameter to display the MAC-based access control function state of ports on the switch. • *<portlist>* - Enter a port or list of ports to be displayed. • *all* – Choose to display all ports. Entering this command without any parameters will display the global settings of the MAC_based access control feature.
Restrictions	None.

Example usage:

To display the global settings for the MAC-based Access Control on the Switch.

```
DES-3800:admin#show mac_based_access_control
Command: show mac_based_access_control

MAC Based Access Control
--------------------------------------------
State                    : Disabled
Method                   : Local
Password                 : default
Guest VLAN               :
Guest VLAN Member Ports  :

DES-3800:admin#
```

Example usage:

To display the running state of ports 1-5 for the MAC-based Access Control on the Switch.

```
DES-3800:admin#show mac_based_access_control ports 1-5
Command: show mac_based_access_control ports 1-5

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

DES-3800:admin#
```

create mac_based_access_control guest_vlan

Purpose	Used to configure a previously created Guest VLAN as a MAC-based access control guest VLAN.
Syntax	**create mac_based_access_control guest_vlan <vlan_name 32>**
Description	This command is used to configure a previously created guest VLAN as a MAC-based access control guest VLAN. This VLAN must have been previously created as first a VLAN, and then a Guest VLAN. Only a VLAN that has been set as a Guest VLAN can be set as a MAC-based access control Guest VLAN.
Parameters	*<vlan_name 32>* - Enter the name of the previously created Guest VLAN to be nominated as the MAC-based access control Guest VLAN.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure a Guest VLAN as a MAC-based Access Control Guest VLAN.

```
DES-3800:admin#create mac_based_access_control guest_vlan Triton
Command: create mac_based_access_control guest_vlan Triton

Success.

DES-3800:admin#
```

config mac_based access_control guest_vlan

Purpose	Used to set the ports for a previously created MAC-based access control Guest VLAN.
Syntax	**config mac_based access_control guest_vlan ports <portlist>**
Description	This command is used to configure ports to be used for MAC-Based Access Control within the Guest VLAN. These ports must have been previously set for the Guest VLAN.
Parameters	*ports <portlist>* - Enter the ports within the Guest VLAN that will be used for the MAC-based access control feature.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the ports of a MAC-based Access Control Guest VLAN.

```
DES-3800:admin#config mac_based_access_control guest_vlan ports 1-
5
Command: config mac_based_access_control guest_vlan ports 1-5

Success.

DES-3800:admin#
```

delete mac_based_access_control guest_vlan

Purpose	Used to delete a MAC-based access control Guest VLAN.
Syntax	**delete mac_based_access_control guest_vlan**
Description	This command is used to delete a MAC-Based Access Control Guest VLAN.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete a MAC-based Access Control Guest VLAN.

```
DES-3800:admin#delete mac_based_access_control guest_vlan
Command: delete mac_based_access_control guest_vlan

Success.

DES-3800:admin#
```

create mac_based_access_control_local mac

Purpose	Used to set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch
Syntax	**create mac_based_access_control_local mac <macaddr> vlan <vlan_name 32>**
Description	This command is used to set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this table, it will be placed in the VLAN associated with it here. The switch administrator may enter up to 1024 MAC addresses to be authenticated using the local method configured here.
Parameters	*mac <macaddr>* - Enter the MAC address which is to be authenticated locally by the Switch, when queried. *<vlan_name 32>* - Enter the name of the VLAN where this MAC address will be placed after a successful authentication.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enter a MAC address into this local database which is to be locally authenticated by the Switch, and the VLAN where it is to be placed after successful authentication:

```
DES-3800:admin#create mac_based_access_control_local mac 00-01-0A-3B-00-06
vlan Triton
Command: create mac_based_access_control_local mac 00-01-0A-3B-00-06 vlan
Triton

Success.

DES-3800:admin#
```

config mac_based_access_control_local mac

Purpose	Used to modify a MAC addresses and its corresponding target VLAN within the local MAC-based access control authentication database.
Syntax	**config mac_based_access_control_local mac <macaddr> vlan <vlan_name 32>**
Description	This command is modify a MAC addresses and its corresponding target VLAN within the local MAC-based access control authentication database. Once a queried MAC address is matched in this table, it will be placed in the VLAN associated with it here. The switch administrator may enter up to 1024 MAC addresses to be authenticated using the local method configured here.
Parameters	*mac <macaddr>* - Enter the MAC address which is to be authenticated locally by the Switch, when queried. *<vlan_name 32>* - Enter the name of the VLAN where this MAC address will be placed after a successful authentication.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To modify a MAC address into this local database which is to be locally authenticated by the Switch, and the VLAN where it is to be placed after successful authentication:

```
DES-3800:admin#config mac_based access_control_local mac 00-01-0A-3B-00-06
vlan default
Command: config mac_based access_control_local mac 00-01-0A-3B-00-06 vlan
default

Success.

DES-3800:admin#
```

delete mac_based_access_control_local mac

Purpose	Used to delete a MAC addresses from the local MAC-based access control authentication database.
Syntax	**delete mac_based access_control_local [mac <macaddr> | vlan <vlan_name 32>]**
Description	This command is delete a MAC addresses from the local MAC-based access control authentication database. Once a queried MAC address is matched in this table, it will be placed in the VLAN associated with it here. The switch administrator may enter up to 1024 MAC addresses to be authenticated using the local method configured here.
Parameters	*mac <macaddr>* - Enter the MAC address which is to be deleted from the local MAC-based access control authentication database. *<vlan_name 32>* - Enter the name of the VLAN which is to be deleted from the local MAC-Based access control authentication database.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete a MAC address into this local database which is to be locally authenticated by the Switch, and the VLAN where it is to be placed after successful authentication:

```
DES-3800:admin#delete mac_based_access_control_local mac 00-01-0A-
3B-00-06
Command: delete mac_based_access_control_local mac 00-01-0A-3B-00-
06
```

```
Success.

DES-3800:admin#
```

show mac_based access_control_local mac

Purpose	Used to display the local MAC-based access control authentication database.
Syntax	**show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32>]}**
Description	This command is used to display the local MAC-based access control authentication database.
Parameters	*mac <macaddr>* - Enter the MAC address within the local MAC-based access control authentication database to be displayed. *<vlan_name 32>* - Enter the name of the VLAN within the local MAC-based access control authentication database to be displayed, with its corresponding MAC addresses. Entering no parameters will display all entries located in the local MAC-based access control authentication database, along with their corresponding target VLANs.
Restrictions	None.

Example usage:

To display a MAC address entry located within the local MAC-based access control authentication database.

```
DES-3800:admin#show mac_based_access_control_local mac 00-01-0A-3B-00-06
Command: show mac_based_access_control_local mac 00-01-0A-3B-00-06

MAC Address                VLAN Name
-----------------          ------------------
00-01-0A-3B-00-06          Triton

Total Entries: 1

DES-3800:admin#
```

To display MAC address entries located within the local MAC-based access control authentication database by VLAN.

```
DES-3800:admin#show mac_based_access_control_local vlan Triton
Command: show mac_based_access_control_local mac vlan Triton

MAC Address                VLAN Name
-----------------          ------------------
00-01-0A-3B-00-06          Triton
00-02-0A-3B-00-02          Triton

Total Entries: 2

DES-3800:admin#
```

To display all MAC address entries located within the local MAC-based access control authentication database.

```
DES-3800:admin#show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address                VLAN Name
-----------------          -----------------
00-01-0A-3B-00-06          Triton
00-02-0A-3B-00-02          Triton
01-03-0B-3A-00-02          default
00-02-03-4B-01-02          default

Total Entries: 4

DES-3800:admin#
```

show mac_based_access_control auth_mac

Purpose	Used to display the MAC-based access control current authentication status.
Syntax	**show mac_based_access_control auth_mac {ports <portlist>}**
Description	This command is used to display current authentication process of MAC addresses located in the local MAC-based access control authentication database, by port.
Parameters	*ports <portlist>* - Enter a port or portlist by which to view the current authenticating process of MAC addresses located on that port.
Restrictions	None.

Example usage:

To display the current authentication process of MAC addresses on port 1.

```
DES-3800:admin#show mac_based_access_control auth_mac
Command: show mac_based_access_control_local auth_mac

Port number : 1
Index    MAC Address            Auth State     VLAN Name
---      ----------             ---------     -----------
1        00-00-01-02-03-A2      Authenticating    default
2        00-03-09-18-10-01      Authenticating    default
3        00-05-5D-ED-84-EA      Authenticating    default
4        00-0D-0B-4E-A0-F7      Authenticating    default
5        00-0D-60-8F-49-38      Authenticating    default
6        00-0E-A6-8E-C1-B7      Authenticating    default
7        00-10-4B-69-F4-AD      Authenticating    default
8        00-11-D8-DA-CE-0B      Authenticating    default
9        00-15-E9-C4-FD-A0      Authenticating    default
10       00-54-85-77-00-03      Authenticating    default
11       00-80-C8-39-41-DD      Authenticating    default
12       00-80-C8-58-72-1B      Authenticating    default
13       00-80-C8-DF-E8-02      Authenticating    default
14       00-A0-C9-01-01-23      Authenticating    default
15       00-E0-18-45-C7-28      Authenticating    default
16       00-E0-18-FB-43-3E      Authenticating    default

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

57

PIM COMMANDS

PIM or *Protocol Independent Multicast* is a method of forwarding traffic to multicast groups over the network using any pre-existing unicast routing protocol, such as RIP or OSPF, set on routers within a multicast network. The xStack DES-3800 switch series supports two types of PIM, Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).

PIM-SM

PIM-SM or *Protocol Independent Multicast – Sparse Mode* is a method of forwarding multicast traffic over the network only to multicast routers who actually request this information. Unlike most multicast routing protocols which flood the network with multicast packets, PIM-SM will forward traffic to routers who are explicitly a part of the multicast group through the use of a Rendezvous Point (RP). This RP will take all requests from PIM-SM enabled routers, analyze the information and then returns multicast information it receives from the source, to requesting routers within its configured network. Through this method, a distribution tree is created, with the RP as the root. This distribution tree holds all PIM-SM enabled routers within which information collected from these router is stored by the RP.

Two other types of routers also exist with the PIM-SM configuration. When many routers are a part of a multiple access network, a Designated Router (DR) will be elected. The DR's primary function is to send Join/Prune messages to the RP. The router with the highest priority on the LAN will be selected as the DR. If there is a tie for the highest priority, the router with the higher IP address will be chosen.

The third type of router created in the PIM-SM configuration is the Boot Strap Router (BSR). The goal of the Boot Strap Router is to collect and relay RP information to PIM-SM enabled routers on the LAN. Although the RP can be statically set, the BSR mechanism can also determine the RP. Multiple Candidate BSRs (C-BSR) can be set on the network but only one BSR will be elected to process RP information. If it is not explicitly apparent which C-BSR is to be the BSR, all C-BSRs will emit Boot Strap Messages (BSM) out on the PIM-SM enabled network to determine which C-BSR has the higher priority and once determined, will be elected as the BSR. Once determined, the BSR will collect RP data emanating from candidate RPs on the PIM-SM network, compile it and then send it out on the land using periodic Boot Strap Messages (BSM). All PIM-SM Routers will get the RP information from the Boot Strap Mechanism and then store it in their database.

Discovering and Joining the Multicast Group

Although Hello packets discover PIM-SM routers, these routers can only join or be "pruned" from a multicast group through the use of Join/Prune Messages exchanged between the DR and RP. Join/Prune Messages are packets relayed between routers that effectively state which interfaces are, or are not to be receiving multicast data. These messages can be configured for their frequency to be sent out on the network and are only valid to routers if a Hello packet has first been received. A Hello packet will simply state that the router is present and ready to become a part of the RP's distribution tree. Once a router has accepted a member of the IGMP group and it is PIM-SM enabled, the interested router will then send an explicit Join/Prune message to the RP, which will in turn route multicast data from the source to the interested router, resulting in a unidirectional distribution tree for the group. Multicast packets are then sent out to all nodes on this tree. Once a prune message has been received for a router that is a member of the RP's distribution tree, the router will drop the interface from its distribution tree.

Distribution Trees

Two types of distribution trees can exist within the PIM-SM protocol, a Rendezvous-Point Tree (RPT) and a Shortest Path Tree (SPT). The RP will send out specific multicast data that it receives from the source to all outgoing interfaces enabled to receive multicast data. Yet, once a router has determined the location of its source, an SPT can be created, eliminating hops between the source and the destination, such as the RP. This can be configured by the switch administrator by setting the multicast data rate threshold. Once the threshold has been passed, the data path will switch to the SPT. Therefore, a closer link can be created between the source and destination, eliminating hops previously used and shortening the time a multicast packet is sent from the source to its final destination.

Register and Register Suppression Messages

Multicast sources do not always join the intended receiver group. The first hop router (DR) can send multicast data without being the member of a group or having a designated source, which essentially means it has no information about how to relay this information to the RP distribution tree. This problem is alleviated through Register and Register-Stop messages. The first multicast packet received by the DR is encapsulated and sent on to the RP which in turn removes the encapsulation and sends the packet on down the RP distribution tree. When the route has been established, a SPT can be created to directly connect routers to the source, or the multicast traffic flow can begin, traveling from the DR to the RP. When the latter occurs, the same packet may be sent twice, one type encapsulated, one not. The RP will detect this flaw and then return a Register Suppression message to the DR requesting it to discontinue sending encapsulated packets.

Assert Messages

At times on the PIM-SM enabled network, parallel paths are created from source to receiver, meaning some receivers will receive the same multicast packets twice. To improve this situation, Assert messages are sent from the receiving device to both multicast sources to determine which single router will send the receiver the necessary multicast data. The source with the shortest metric (hop count) will be elected as the primary multicast source. This metric value is included within the Assert message.

PIM-DM

The *Protocol Independent Multicast - Dense Mode* (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth as PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead.

The PIM-DM multicast routing protocol is assumes that all downstream routers want to receive multicast messages and relies upon explicit prune messages from downstream routers to remove branches from the multicast delivery tree that do not contain multicast group members.

PIM-DM has no explicit ‘join’ messages. It relies upon periodic flooding of multicast messages to all interfaces and then either waiting for a timer to expire (the **Join/Prune Interval**) or for the downstream routers to transmit explicit ‘prune’ messages indicating that there are no multicast members on their respective branches. PIM-DM then removes these branches (‘prunes’ them) from the multicast delivery tree.

Because a member of a pruned branch of a multicast delivery tree may want to join a multicast delivery group (at some point in the future), the protocol periodically removes the ‘prune’ information from its database and floods multicast messages to all interfaces on that branch. The interval for removing ‘prune’ information is the **Join/Prune Interval**.

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

Command	Parameters
enable pim	
disable pim	
config pim	[[ipif <ipif_name 12> | all] {hello <sec 1-18724> | jp_interval <sec 1-18724> | state [enable | disable] | mode [dm | sm] | dr_priority <unsigned_int 0 – 4294967294>}
config pim register_probe_time	<value 1-127>
config pim register_suppression_time	<value 3-255>
create pim crp group	<ip_addr/netmask> rp <ipif_name 12>
delete pim crp group	<ip_addr/netmask>
config pim crp	{holdtime <value 0-255> | priority <value 0-255> | wildcard_prefix_cnt [0 | 1]}
create pim static_rp group	<ip_addr/netmask> rp <ipaddr>
delete pim static_rp group	<ip_addr/netmask>
show pim static_rp	
config pim rp_spt_threshold	[<value 0-256> | infinity]
config pim last_hop_spt_threshold	[<value 0-256> | infinity]
show pim rpset	
show pim crp	
config pim cbsr	[ipif <ipif_name 12> {priority [-1 | <value 0-255>]} | hash_masklen <value 0-32> | bootstrap_period <value 1-255>]
show pim cbsr	{ipif <ipif_name 12>}
show pim	{ipif <ipif_name 12>}

Command	Parameters
show pim neighbor	{ipif <ipif_name 12> | ipaddress <network_address>}
show pim ipmroute	
create pim register_checksum_include_data rp_address	<ipaddr>
delete pim register_checksum_include_data rp_address	<ipaddr>
show pim register_checksum_include_data_rp_list	
show pim active_rp	{group <multicast_ipaddr>}

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

enable pim

Purpose	Used to enable the PIM function on the Switch.
Syntax	**enable pim**
Description	This command will enable PIM for the Switch. PIM settings must first be configured for specific IP interfaces using the **config pim** command.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To enable PIM as previously configured on the Switch:

```
DES-3800:admin#enable pim
Command: enable pim

Success.

DES-3800:admin#
```

disable pim

Purpose	Used to disable PIM function on the Switch.
Syntax	**disable pim**
Description	This command will disable PIM for the Switch. Any previously configured PIM settings will remain unchanged and may be enabled at a later time with the **enable pim** command.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To disable PIM on the Switch:

```
DES-3800:admin#disable pim
Command: disable pim

Success.

DES-3800:admin#
```

config pim	
Purpose	Used to configure the parameters for the PIM protocol.
Syntax	**config pim [[ipif <ipif_name 12> | all] {hello <sec 1-18724> | jp_interval <sec 1-18724> | state [enable | disable] | mode [dm | sm] | dr_priority <unsigned_int 0 – 4294967294>}]**
Description	This command will configure the general settings for the PIM protocol per IP interface, including choice of PIM mode, Designated Router priority and various timers.
Parameters	*ipif <ipif_name 12>* - Enter an IP interface for which to configure the PIM settings. This name cannot exceed 12 alphanumeric characters. *all* – Select this parameter to configure PIM settings for all IP interfaces on the Switch. *hello <sec 1-18724>* - Used to set the interval time between the sending of Hello Packets from this IP interface to neighboring routers one hop away. These Hello packets are used to discover other PIM enabled routers and state their priority as the Designated Router (DR) on the PIM enabled network. The user may state an interval time between 1 – 18724 seconds with a default interval time of 30 seconds. *jp_interval <sec 1-18724>* - This field will set the interval time between the sending of Join/Prune packets stating which multicast groups are to join the PIM enabled network and which are to be removed or “pruned” from that group. The user may state an interval time between 1 – 18724 seconds with a default interval time of 30 seconds. *state [enable* | *disable]* - Used to enable or disable PIM for this IP interface. The default is Disabled. *mode [dm* | *sm]* - Used to select the type of PIM protocol to use, Sparse Mode (SM) or Dense Mode (DM). The default setting is DM. *dr_priority <unsigned_int 0 – 4294967294>* - Enter the priority of this IP interface to become the Designated Router for the multiple access network. The user may enter a DR priority between 0 and 4,294,967,294 with a default setting of 1.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the PIM settings for an IP interface:

```
DES-3800:admin#config pim ipif Trinity hello 60 jp_interval 60
state enable mode sm dr_priority 2
Command: config pim ipif Trinity hello 60 jp_interval 60 state
enable mode sm dr_priority 2

Success.

DES-3800:admin#
```

config pim register_probe_time

Purpose	Used to set a time to send a probe message from the DR to the RP before the Register Suppression time expires.
Syntax	**config pim register_probe_time <value 1-127>**
Description	This command is used to set a time to send a probe message from the DR to the RP before the Register Suppression time expires. If a Register Stop message is received by the DR, the Register Suppression Time will be restarted. If no Register Stop message is received within the probe time, Register Packets will be resent to the RP. This command is for PIM-SM configurations only.
Parameters	*<value 1-127>* - Configure this field to set a time to send a probe message from the DR to the RP before the Register Suppression time expires. The user may configure a time between 1-127 seconds with a default setting of 5 seconds.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the register probe time:

```
DES-3800:admin#config pim register_probe_time 5
Command: config pim register_probe_time 5

Success.

DES-3800:admin#
```

config pim register_suppression_time

Purpose	Used to configure the interval between the sending of register packets for the PIM protocol.
Syntax	**config pim register_suppression_time <value 3-255>**
Description	This command is to be configured for the first hop router from the source. After this router sends out a register message to the RP, and the RP replies with a register stop message, it will wait for the time configured here to send out another register message to the RP. This command is for PIM-SM configurations only.
Parameters	*<value 3-255>* - The user may set an interval time between 3-255 with a default setting of 60 seconds for the sending of register suppression time packets. The default value is 60 seconds.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the register suppression time:

```
DES-3800:admin#config pim register_suppression_time 15
Command: config pim register_suppression time_15

Success.

DES-3800:admin#
```

NOTE: The Probe time value must be less than half of the Register Suppression Time value. If not, the administrator will be presented with a Fail message.

create pim crp

Purpose	To enable the Switch to become a candidate to be the Rendezvous Point (RP).
Syntax	**create pim crp group <ip_addr/netmask> rp <ipif_name 12>**
Description	This command will set the parameters for the switch to become a candidate RP. This command is for PIM-SM configurations only.
Parameters	*group <ip_addr/netmask>* - Enter the multicast group address for this switch to become a Candidate RP. This address must be a class D address. *rp <ipif_name 12>* - Enter the name of the PIM-SM enabled interface the switch administrator wishes to become the CRP for this group.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To create an IP interface to become a Candidate RP on the Switch:

```
DES-3800:admin#create pim crp group 231.0.0.1/32 rp Trinity
Command: create pim crp group 231.0.0.1/32 rp Trinity

Success.

DES-3800:admin#
```

delete pim crp

Purpose	To disable the Switch in becoming a possible candidate to be the Rendezvous Point (RP).
Syntax	**delete pim crp group <ip_addr/netmask>**
Description	This command remove the switch’s status of Candidate RP. This command is for PIM-SM configurations only.
Parameters	*group <ip_addr/netmask>* - Enter the multicast group address for this switch to be removed from being a Candidate RP. This address must be a class D address.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To delete an IP interface from becoming a Candidate RP on the Switch:

```
DES-3800:admin#delete pim crp group 231.0.0.1/32
Command: delete pim crp group 231.0.0.1/32

Success.

DES-3800:admin#
```

config pim crp

Purpose	To configure the Candidate RP settings that will determine the RP.
Syntax	**config pim crp {holdtime <value 0-255> | priority <value 0-255> | wildcard_prefix_cnt [0 | 1]}**
Description	This command will configure parameters regarding the Candidate RP on the Switch, including hold time, priority and wildcard prefix count. This command is for PIM-SM configurations only.
Parameters	*holdtime <value 0-255>* - This field is used to set the time Candidate RP (CRP) advertisements are valid on the PIM-SM enabled network. If CRP advertisements are not received by the BSR within this time frame, the CRP is removed from the list of candidates. The user may set a time between 0 - 255 seconds with a default setting of 150 seconds. An entry of 0 will send out one advertisement that states to the BSR that it should be immediately removed from CRP status on the PIM-SM network. *priority <value 0-255>* - Enter a priority value to determine which CRP will become the RP for the distribution tree. This priority value will be included in the router's CRP advertisements. A lower value means a higher priority, yet, if there is a tie for the highest priority, the router having the higher IP address will become the RP. The user may set a priority between 0 – 255 with a default setting of 0. *wildcard_prefix_cnt [0 | 1]* - The user may set the Prefix Count value of the wildcard group address here by choosing a value between 0 and 1 with a default setting of 0.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure the Candidate RP settings for the multiple access network:

```
DES-3800:admin#config pim crp holdtime 150 priority 2
wildcard_prefix_cnt 0
Command: config pim crp holdtime 150 priority 2
wildcard_prefix_cnt 0

Success.

DES-3800:admin#
```

create pim static_rp

Purpose	Used to enter the multicast group IP address used in identifying the Rendezvous Point (RP).
Syntax	**create pim static_rp group <ip_addr/netmask> rp <ipaddr>**
Description	This command will enter the multicast group IP address which will be used to identify the RP. This entry must be a class D IP address. This command is for PIM-SM configurations only.
Parameters	*group <ip_addr/netmask>* - Enter the multicast group IP address used in determining the Static RP. This address must be a class D IP address. *rp <ipaddr>* - Enter the IP address of the RP the switch administrator wishes to become the Static RP for this group.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To create the settings to determine a static RP:

```
DES-3800:admin#create pim static_rp group 231.0.0.1/32 rp
11.1.1.1
Command: create pim static_rp group 231.0.0.1/32 rp
11.1.1.1

Success.

DES-3800:admin#
```

delete pim static_rp

Purpose	To remove the multicast group IP address used in identifying the Rendezvous Point (RP).
Syntax	**delete pim static_rp group <ip_addr/netmask>**
Description	This command will remove the multicast group IP address used in identifying the Rendezvous Point (RP). This command is for PIM-SM configurations only.
Parameters	*group <ip_addr/netmask>* - Enter the multicast group IP address used in identifying the Rendezvous Point (RP). This address must be a class D address.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To remove the multicast group IP address used in identifying the Rendezvous Point (RP).:

```
DES-3800:admin#delete pim static_rp group 231.0.0.1/32
Command: delete pim static_rp group 231.0.0.1/32

Success.

DES-3800:admin#
```

show pim static_rp

Purpose	To show the Static Rendezvous Point (RP) settings.
Syntax	**show pim static_rp**
Description	This command will display the Static Rendezvous Point (RP) settings. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	None.

Usage example:

To display the static RP settings as configured for the multiple access network:

```
DES-3800:admin#show pim static_rp
Command: show pim static_rp

PIM Static RP Table

Group                   RP Address
-------------           -----------
```

```
224.0.0.1/4             11.1.1.254
239.0.0.1/32            31.1.1.1
239.0.0.2/32            31.1.1.12
239.0.0.3/32            31.1.1.123

Total entries: 4


DES-3800:admin#
```

config pim rp_spt_threshold

Purpose	Used to configure the threshold of register packets needed to enable the Shortest Path Tree (SPT).
Syntax	**config pim rp_spt_threshold [<value 0-256> | infinity]**
Description	This command will set the threshold of register packets needed to enable the Shortest Path Tree (SPT). When the amount of register packets per second reaches the configured threshold, it will trigger the RP to switch to an SPT, between the RP and the first hop router. This command is for PIM-SM configurations only.
Parameters	*<value 0–256>* - Enter a value between 0 – 256 to determine the number of packets per second needed to Switch the path to a SPT. The default setting is 0. 0 denotes the router will enter the SPT immediately. *infinity* - An entry of *infinity* will disable the RP from entering an SPT.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To set the SPT threshold:

```
DES-3800:admin# config pim rp_spt_threshold 200
Command: config pim rp_spt_threshold 200

Success.

DES-3800:admin#
```

config last_hop_spt_threshold

Purpose	Used to configure the packet threshold that the last hop router in the RP tree will use to change its path to a SPT.
Syntax	**config last_hop_spt_threshold [<value 0-256> | infinity]**
Description	This command will configure the threshold of multicast data packets needed to change the last hop router’s distribution tree to a SPT. When the amount of multicast packets per second reaches the configured threshold, the last hop router will change its distribution tree to a (Shortest Path Tree) SPT. This command is for PIM-SM configurations only.
Parameters	*<value 0 –256>* - Enter a value between 0 – 256 to determine the number of packets per second needed to Switch the path to a SPT. The default setting is 0. 0 denotes that the router will immediately enter the SPT. *infinity* - An entry of *infinity* will disable the last hop router from entering an SPT.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure the last hop router to never enter an SPT:

```
DES-3800:admin#config last_hop_spt_threshold 0
Command: config last_hop_spt_threshold 0

Success.

DES-3800:admin#
```

show pim rpset

Purpose	Used to display the RP Set of the Switch.
Syntax	**show pim rpset**
Description	This command will display the information regarding the RP Set learned by the BSR. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	None.

Usage example:

To view the RP Set information:

```
DES-3800:admin# show pim rpset
Command: show pim rpset

Bootstrap Router: 12.43.51.81

Group Address   RP Address   Holdtime   Expired Time   Type
-------------   -----------  ---------  ------------   ------
224.0.0.1/4     31.43.51.81  150        107

Total Entries: 1

DES-3800:admin#
```

show pim crp

Purpose	Used to display the Candidate RP settings on the Switch, along with CRP parameters configured for the Switch.
Syntax	**show pim crp**
Description	This command will display the settings for Candidate RPs that are accessible to the switch. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To view the CRP settings:

```
DES-3800:admin# show pim crp
Command: show pim crp

PIM Candidate-RP Table

C-RP Holdtime                : 150
C-RP Priority                : 2
C-RP wildcard prefix count   : 0
```

```
Group                        Interface
----------------             -------------
224.0.0.1/4                  Trinity

DES-3800:admin#
```

config pim cbsr

Purpose	Used to configure the settings for the Candidate Bootstrap Router and the priority of the selected IP interface to become the Boot Strap Router (BSR) for the PIM-SM network domain.
Syntax	**config pim cbsr [ipif <ipif_name 12> {priority [-1 | value 0-255>]} | hash_masklen <value 0-32> | bootstrap_period <value 1-255>]**
Description	This command will configure the settings for the Candidate BSR. The Boot Strap Router holds the information which determines which router on the network is to be elected as the RP for the multicast group and then to distribute RP information to other PIM-SM enabled routers. This command is for PIM-SM configurations only.
Parameters	*ipif <ipif_name 12>* - Enter the ipif name of the interface to become the CBSR. *priority [-1 | value 0-255>]* - Used to state the Priority of this IP Interface to become the BSR. The user may select a priority between -1 to 255. An entry of -1 states that the interface will be disabled to be the BSR. *hash_masklen <value 0-32>* Enter a hash mask length, which will be used with the IP address of the candidate RP and the multicast group address, to calculate the hash algorithm used by the router to determine which CRP on the PIM-SM enabled network will be the RP. The user may select a length between 0 –32 with a default setting of 30. This parameter must be configured separately from the ipif settings of this command. See the examples below for a better understanding. *bootstrap_period <value 1-255>* - Enter a time period between 1-255 to determine the interval the Switch will send out Boot Strap Messages (BSM) to the PIM enabled network. The default setting is 60 seconds. This parameter must be configured separately from the ipif settings of this command. See the examples below for a better understanding.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To configure the settings for an IP interface to become a CBSR on the multiple access network:

```
DES-3800:admin#config pim cbsr ipif Trinity priority 4
Command: config pim cbsr ipif Trinity priority 4

Success.

DES-3800:admin#
```

Usage example:

To configure the hash mask length for the CBSR:

```
DES-3800:admin#config pim cbsr hash_masklen 30
Command: config pim cbsr hash_masklen 30

Success.

DES-3800:admin#
```

Usage example:

To configure the bootstrap period for the CBSR:

```
DES-3800:admin#config pim cbsr bootstrap_period 60
Command: config pim cbsr bootstrap_period 60

Success.

DES-3800:admin#
```

show pim cbsr

Purpose	Used to display the Candidate BSR settings of the switch, along with CBSR parameters configured for the Switch.
Syntax	**show pim cbsr {ipif <ipif_name12>}**
Description	This command will display the settings for Candidate BSRs that are accessible to the switch. This command is for PIM-SM configurations only.
Parameters	*<ipif_name 12>* - Enter the name of the IP interface for which to display settings. Entering no name will display all CBSRs.
Restrictions	None.

Usage example:

To view the CBSR settings:

```
DES-3800:admin# show pim cbsr
Command: show pim cbsr

PIM Candidate-BSR Table

C-BSR Hash Mask Len         : 30
C-BSR Bootstrap Period      : 2

Interface            IP Address                Priority
------------------   -----------               --------
Trinity              11.1.1.1/8                4
System               10.53.13.30/8             -1 (disabled)

DES-3800:admin#
```

show pim

Purpose	Used to display the PIM settings, along with PIM parameters configured for the Switch.
Syntax	**show pim {ipif <ipif_name12>}**
Description	This command will display the settings for the PIM function that are accessible to the switch.
Parameters	*<ipif_name 12>* - Enter the name of the IP address for which to display settings. Entering no name will display all PIM IP interfaces.
Restrictions	None.

Usage example:

To view the PIM settings:

```
DES-3800:admin# show pim
Command: show pim

PIM Global State                                : Enabled
Last Hop SPT Threshold    : 0  packet per second (switch to SPT tree immediately)
RP SPT threshold          : 0  packet per second (switch to SPT tree immediately)
Register Probe Time       : 5
Register Suppression Time : 60

PIM Interface Table

                                Designated   Hello        J/P
Interface       IP Address      Router      Interval     Interval  Mode State
----------      ----------     ----------    --------     --------  ---- -------
Trinity         11.1.1.1/8     10.53.13.30   30           60        DM   Disabled
System          10.53.13.30/8  11.1.1.1      60           60        SM   Enabled

Total Entries: 2

DES-3800:admin#
```

show pim neighbor

Purpose	Used to display PIM neighbors of the Switch.
Syntax	**show pim neighbor {ipif <ipif_name12> | ipaddress <network_address>}**
Description	This command will display the PIM neighbor table for the Switch.
Parameters	*<ipif_name 12>* - Enter the name of the IP interface for which to display PIM information regarding PIM neighbors. *ipaddress <network_address>* - Enter the IP address of a PIM neighbor for which to display information. Adding no parameters to this command will display all PIM neighbors that probed the Switch.
Restrictions	None.

Usage example:

To view the PIM neighbors:

```
DES-3800:admin# show pim neighbor
Command: show pim neighbor

PIM Neighbor Address Table

Interface Name         Neighbor Address    Expired Time
--------------         ----------------    ------------
n10                    10.20.6.251         79

Total Entries: 1

DES-3800:admin#
```

show pim ipmroute

Purpose	Used to display the PIM IP Multicast Route Table on the Switch.
Syntax	**show pim ipmroute**
Description	This command will display the PIM IP Multicast Route Table on the Switch. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	None.

Usage example:

To view the PIM routes:

```
DES-3800:admin# show pim ipmroute
Command: show pim ipmroute

PIM IP Multicast Route Table

UA = Upstream AssertTimer
AM = Assert Metric
AMPref = Assert MetricPref
ARB    = Assert RPTBit

Group Address   Source Address     UA    AM     AMPref      ARB      Flag      Type
-------------   ----------------   ----  ----   ------     ------    ----      -------
224.0.1.1       31.43.51.81/32      0     0       0           0       rpt        (*.G)
224.0.1.24      10.54.81.250/32     0     0       0           0       spt        (S.G)
224.0.1.24      10.55.68.64/32      0     0       0           0       spt        (S.G)
224.0.1.24      31.43.51.81/32      0     0       0           0       rpt        (*.G)
229.55.150.208  10.6.51.1/32        0     0       0           0       spt        (S.G)
229.55.150.208  10.38.45.151/32     0     0       0           0       spt        (S.G)
229.55.150.208  10.38.45.192/32     0     0       0           0       spt        (S.G)
229.55.150.208  10.50.93.100/32     0     0       0           0       spt        (S.G)
229.55.150.208  10.51.16.1/32       0     0       0           0       spt        (S.G)
229.55.150.208  10.59.23.10/32      0     0       0           0       spt        (S.G)
229.55.150.208  31.43.51.81/32      0     0       0           0       rpt        (*.G)
239.192.0.1     31.43.51.81/32      0     0       0           0       rpt        (*.G)

Total Entries: 12

DES-3800:admin#
```

create pim register_checksum_include_data

Purpose	Used to set the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets.
Syntax	**create pim register_checksum_include_data rp_ address <ipaddr>**
Description	This command will set the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets. This command is for PIM-SM configurations only.
Parameters	*rp_address <ipaddr>* - Enter the IP address of the RP that will verify checksums included with Registered packets.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To create an RP to which the Switch will send Register packets to and create checksums to be included with the data in Registered packets:

```
DES-3800:admin# create pim register_checksum_include_data rp_
address 11.1.1.1
Command: create pim register_checksum_include_data rp_ address
11.1.1.1

Success.

DES-3800:admin#
```

delete pim register_checksum_include_data

Purpose	Used to disable the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets.
Syntax	**delete pim register_checksum_include_data rp_ address <ipaddr>**
Description	This command will disable the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets. This command is for PIM-SM configurations only.
Parameters	*rp_address <ipaddr>* - Enter the IP address of the RP that will discontinue sending Register packets to and create checksums to be included with the data in Registered packets.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage example:

To delete RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets:

```
DES-3800:admin#delete pim register_checksum_include_data rp_
address 11.1.1.1
Command: delete pim register_checksum_include_data rp_ address
11.1.1.1

Success.

DES-3800:admin#
```

show pim register_checksum_include_data_rp_list

Purpose	Used to display RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets.
Syntax	**show pim register_checksum_include_data_rp_list**
Description	This command will display RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets. This command is for PIM-SM configurations only.
Parameters	None*.*
Restrictions	None.

Usage example:

To show the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets:

```
DES-3800:admin# show pim register_checksum_include_data_rp_ list
Command: show pim register_checksum_include_data_rp_ list

RP Address
-------------------------------------------
11.1.1.1

Total Entries: 1

DES-3800:admin#
```

show pim active_rp

Purpose	Used to display currently active RPs that have been chosen form the RP Set table.
Syntax	**show pim active_rp {group <multicast_ipaddr>}**
Description	This command will display currently active RPs that have been chosen from the RP Set table, which are relaying multicast data.
Parameters	*group <multicast_ipaddr>* - Enter the multicast group IP address used in identifying the Rendezvous Point (RP). This address must be a class D address.
Restrictions	None.

Usage example:

To show the currently active RPs that have been chosen from the RP Set table:

```
DES-3800:admin# show pim active_rp
Command: show pim active_rp

Group Address               RP Address
-----------------          ----------------------
225.1.1.2                   172.24.5.6
255.1.2.3                   172.24.5.6
235.5.6.7                   152.2.3.4

Total Entries: 3

DES-3800:admin#
```

58

LOOPBACK INTERFACE COMMANDS

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

Command	Parameters
create loopback ipif	<ipif_name 12> <ipaddr> {state [enable | disable]}
delete loopback ipif	[<ipif_name 12> | all]
config loopback ipif	<ipif_name 12> {ipaddress <ipaddr> | state [enable | disable]}
show loopback ipif	{<ipif_name 12>}

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

create loopback ipif

Purpose	Used to create a loopback interface.
Syntax	**create loopback ipif <ipif_name 12> <ipaddr> {state [enable | disable]}**
Description	The create ipif command creates an IP interface on the switch. Loopback interface is a network termination and can't be direct connected to the host. That is the host talks with loopback interface by routing.
Parameters	*ipif* - The name for the IP interface to be created. Maximum length is 12. *ipaddr* - The IP address of this loopback interface. The netmask is always 255.255.255.255 *state* - Allows you to enable or disable the loopback interface.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To create IP address 172.19.10.20 in loopback interface named loopback0.

```
DES-3800:admin# create loopback ipif loopback0
172.19.10.20
Command: create loopback ipif loopback0 172.19.10.20

Success.

DES-3800:admin#
```

delete loopback ipif

Purpose	Used to delete a previously configured loopback interface on the switch.
Syntax	**delete loopback ipif [<ipif_name 12> | all]**
Description	The delete ipif command deletes a previously configured loopback interface on the switch.
Parameters	*ipif_name* - The name of the loopback interface that is to be deleted. *all* - Specifies that all loopback interfaces configured on the switch will be deleted
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To delete the loopback interface loopback0.

```
DES-3800:admin# delete loopback ipif loopback0
Command: delete loopback ipif loopback0

Success.

DES-3800:admin#
```

config loopback ipif

Purpose	Used to configure an loopback IP interface on the switch
Syntax	**config loopback ipif <ipif_name 12> {ipaddress <ipaddr> | state [enable | disable]}**
Description	The config loopback ipif command is used to configure an loopback IP interface on the switch.
Parameters	*ipif_name* - The name of the loopback interface that is to be configured *ipaddress* - IP address of this loopback interface. *state* - Allows you to enable or disable the IP interface.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config the admin status of the loopback interface.

```
DES-3800:admin#config loopback ipif loopback0 state
disable
Command: config loopback ipif loopback0 state disable

Success.

DES-3800:admin#
```

show loopback ipif

Purpose	Used to display the configuration of a loopback IP interface on the switch.
Syntax	**show loopback ipif {<ipif_name 12>}**
Description	The show ipif command displays the configuration of a loopback IP interface on the switch.
Parameters	*ipif_name* - Specifies the name of the loopback IP interface you want to display. If no parameter is specified, the switch will display all loopback IP interfaces.
Restrictions	None.

Usage Example:

To display loopback IP interface settings.

```
DES-3800:admin# show loopback ipif
Command: show loopback ipif

Loopback IP Interface Settings
Interface Name : loopback0
IP Address     : 172.19.10.20
Subnet Mask    : 255.255.255.255
Admin. State   : Enabled
Link Status    : Link UP

Interface Name : loopback1
IP Address     : 30.2.2.2
Subnet Mask    : 255.255.255.255
Admin. State   : Enabled
Link Status    : Link UP

Total Entries : 2

DES-3800:admin#
```

59

DHCP SERVER COMMAND LIST

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

Command	Parameters
create dhcp excluded_address	begin_address <ipaddr> end_address <ipaddr>
delete dhcp excluded_address	[begin_address <ipaddr> end_address <ipaddr> | all]
show dhcp excluded_address	
create dhcp pool	<pool_name 12>
delete dhcp pool	[<pool_name 12> | all]
config dhcp pool network_address	<pool_name 12> <network_address>
config dhcp pool domain_name	<pool_name 12> {<domain_name 64>}
config dhcp pool dns_server	<pool_name 12> {<ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool netbios_name_server	<pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool netbios_node_type	<pool_name 12> [broadcast | peer_to_peer | mixed | hybid]
config dhcp pool default_router	<pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool lease	<pool_name 12> [<day 0-365> <hour 0-23><minute 0-59> | infinite]
config dhcp pool boot_file	<pool_name 12> {<file_name 64>}
config dhcp pool next_server	<pool_name 12> {< ipaddr>}
config dhcp ping_packets	<number 0-10>
config dhcp ping_timeout	<millisecond 10-2000>
create dhcp pool manual_binding	<pool_name 12> < ipaddr> hardware_address <macaddr> {type [ethernet | ieee802]}
delete dhcp pool manual_binding	<pool_name 12> [<ipaddr> | all]
clear dhcp binding	[<pool_name 12> [<ipaddr> | all] | all]
show dhcp binding	{<pool_name 12>}
show dhcp pool	{<pool_name 12>}
show dhcp pool manual_binding	{<pool_name 12>}
enable dhcp_server	
disable dhcp_server	
show dhcp_server	
clear dhcp conflict_ip	[<ipaddr> | all]
show dhcp conflict_ip	{<ipaddr>}

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

create/delete dhcp excluded_address	
Purpose	Specifies the IP addresses that the DHCP server should not assign to DHCP client.
Syntax	**create dhcp excluded_address begin_address < ipaddr > end_address < ipaddr >** **delete dhcp excluded_address [begin_address < ipaddr > end_address < ipaddr > | all]**
Description	The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. You must use this command to specify the IP address that the DHCP server should not assign to clients. This command can be used multiple times in order to define multiple groups of excluded addresses.
Parameters	< *ipaddr* > Start/end addrress of ipaddress range.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To specify the IP address that DHCP server should not assign to clients.

```
DES-3800:admin#create dhcp excluded_address
begin_address 10.10.10.1 end_address 10.10.10.10
Command: create dhcp excluded_address begin_address
10.10.10.1 end_address 10.10.10.10


Success.


DES-3800:admin#
```

show dhcp excluded_address	
Purpose	Display the groups of IP addresses which are excluded from the legal assigned IP address.
Syntax	**show dhcp excluded_address**
Description	The show dhcp excluded_address command displays the configuration of DHCP excluded addreesses
Parameters	None.
Restrictions	None.

Usage Example:

To display the excluded addresses:

```
DES-3800:admin#show excluded_address
Command: show excluded_address

Index  Begin Address    End Address
-----  ---------------  ---------------
1      192.168.0.1      192.168.0.100
2      10.10.10.10      10.10.10.10

Total Entries : 2

DES-3800:admin#
```

create/delete dhcp pool

Purpose	Creates/delete a DHCP pool
Syntax	**create dhcp pool <pool_name 12>** **delete dhcp pool [<pool_name 12> | all]**
Description	You must create a DHCP pool by specifying a name. After you create a DHCP pool, use other DHCP pool configuration command to configure parameters for the pool.
Parameters	*<pool_name 12>* - Pool's name.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To create a DHCP pool:

```
DES-3800:admin#create dhcp pool engineering
Command: create dhcp pool engineering

Success.

DES-3800:admin#
```

config dhcp pool network_addr

Purpose	Specifies the network for the DHCP pool.
Syntax	**config dhcp pool network_addr <pool_name 12> <network_address>**
Description	Specifies the network for the DHCP pool. The addresses in the network are free to be assigned to the DHCP client.. The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/). When the DHCP server receives a request from the client, the server will automatically find a pool to allocate the address. If the request is relayed to the server by the intermediate device, the server will match the gateway IP address carried in the packet against the network of each DHCP pool. The pool which has the longest match will be selected. If the request packet is not through relay, then the server will match the IP address of the IPIF that received the request packet against the network of each DHCP pool.
Parameters	*<pool_name 12>* - Pool's name. *<network_address>* - Ip address that DHCP server may assign to clients.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config address range of the DHCP address pool :

```
DES-3800:admin#config dhcp pool network_addr
engineering 10.10.10.0/24
Command: config dhcp pool network_addr  engineering
10.10.10.0/24


Success.


DES-3800:admin#
```

config dhcp pool domain_name

Purpose	Specifies the domain name for the client if server allocate the address for the client from this pool.
Syntax	**config dhcp pool domain_name <pool_name 12> {<domain_name 64>}**
Description	The domain name configured here will be used as the default domain name by the client. By default, the domain name is empty. If domain name is empty, the domain name information will not be provided to the client .
Parameters	*<pool_name 12>* - Pool's name. *<domain_name 64>* - Domain name of client.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config domain name option of dhcp pool :

```
DES-3800:admin#config dhcp pool domain_name
engineering d_link.com
Command: config dhcp pool domain_name engineering
d_link.com

Success.

DES-3800:admin#
```

config dhcp pool dns_server

Purpose	Specifies the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified in one command line.
Syntax	**config dhcp pool dns_server <pool_name 12> {<ipaddr>} {< ipaddr>} {< ipaddr>}**
Description	If dns server is not specified ,the dns server information will not be provided to the client . If this command are input twice for the same pool, the second command will overwrite the first command.
Parameters	*<pool_name 12>* - Pool's name. *<ipaddr>* - Ip address of DNS server.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config DNS server's IP address :

```
DES-3800:admin#config dhcp pool dns_server engineering
10.10.10.1
Command: config dhcp pool dns_server engineering
10.10.10.1

Success.

DES-3800:admin#
```

config dhcp pool netbios_name_server

Purpose	Specifies the NetBIOS name server that is available to a Microsoft DHCP client. Up to three IP addresses can be specified in one command line.
Syntax	**config dhcp pool netbios_name_server <pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}**
Description	Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks. If netbios name server is not specified,the netbios name server information will not be provided to the client . If this command are input twice for the same pool, the second command will overwrite the first command.
Parameters	*<pool_name 12>* - Pool's name. *<ipaddr>* - Ip address of WINS server.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config WINS server's IP address :

```
DES-3800:admin#config dhcp pool netbios_name_server
engineering 10.10.10.1
Command: config dhcp pool netbios_name_server
engineering 10.10.10.1

Success.

DES-3800:admin#
```

config dhcp pool netbios_node_type

Purpose	Specifies the NetBIOS node type for a Microsoft DHCP client.
Syntax	**config dhcp pool netbios_node_type <pool_name 12> [broadcast | peer_to_peer | mixed | hybid]**
Description	The NetBIOS node type for Microsoft DHCP clients can be one of four settings: broadcast, peer-to-peer, mixed, or hybrid. Use this command to config NetBIOS over TCP/IP device that described in RFC 1001/1002. By default, NetBIOS node type is broadcast.
Parameters	*<pool_name 12>* - Pool's name. *<node_type>* - NetBIOS node type for a Microsoft DHCP client.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To configure NetBIOS node type:

```
DES-3800:admin# config dhcp pool netbios_node_type
engineering hybid
Command: config dhcp pool netbios_node_type
engineering hybid

Success.

DES-3800:admin#
```

config dhcp pool default_router

Purpose	Specifies the IP address of the default router for a DHCP client. Up to three IP addresses can be specified in one command line.
Syntax	**config dhcp pool default_router <pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}**
Description	After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client. If default_router is not specified , the default router information will not be provided to the client. If this command are input twice for the same pool, the second command will overwrite the first command. The default router must be ranged within the network defined for the DHCP pool.
Parameters	*<pool_name 12>* - Pool's name. *<ipaddr>* - Ip address of default router.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To configure default router:

```
DES-3800:admin#config dhcp pool default_router
engineering 10.10.10.1
Command: config dhcp pool default_router engineering
10.10.10.1

Success.

DES-3800:admin#
```

config dhcp pool lease

Purpose	Specifies the duration of the lease.
Syntax	**config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23><minute 0-59> | infinite]**
Description	By default, each IP address assigned by a DHCP server comes with a one-day lease, which is the amount of time that the address is valid.
Parameters	*<pool_name 12>* - Pool's name. *<day 0-365>* - Days of lease. *<hour 0-23>* - Hours of lease. *<minute 0-59>* - Minutes of lease *Infinite* - Means infinite lease.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config lease of a pool:

```
DES-3800:admin#config dhcp pool lease engineering
infinite
Command: config dhcp pool lease engineering infinite

Success.

DES-3800:admin#
```

config dhcp pool boot_file

Purpose	Specifies the name of the file that is used as a boot image.
Syntax	**config dhcp pool boot_file <pool_name 12> {<file_name 64>}**
Description	The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load.
Parameters	*<pool_name 12>* - Pool's name. *< file_name 64>* - File name of boot image.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To configure boot file:

```
DES-3800:admin#config dhcp pool boot_file engineering
boot.had
Command: config dhcp poolboot_file engineering
boot.had

Success.

DES-3800:admin#
```

config dhcp pool next_server

Purpose	Specifies the next server to be used in the DHCP client boot process.
Syntax	**config dhcp pool next_server <pool_name 12> {< ipaddr> }**
Description	The next server used by the DHCP client boot process is typically a TFTP server. It is allowed to specify next_server but not specify the boot file, or specify the boot file but not specifythe next_server.
Parameters	*<pool_name 12>* - Pool's name. *<ipaddr>* - Ip address of next server.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To configure next server:

```
DES-3800:admin#config dhcp pool next_server
engineering 192.168.0.1
Command: config dhcp pool next_server engineering
192.168.0.1

Success.

DES-3800:admin#
```

config dhcp ping_packets

Purpose	Specifies the number of ping packets the DHCP server sends to a the IP address before assigning this address to a requesting client.
Syntax	**config dhcp ping_packets <number 0-10>**
Description	By default, the DHCP server pings a pool address twice before assigning the address to a DHCP client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client. If the ping is answered, the server will discard the current IP address and try another IP address.
Parameters	*<number 0-10>* - Numbers of ping packet. 0 means there is no ping test. The default value is 2.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config ping packets:

```
DES-3800:admin#config dhcp ping_packets 4
Command: config dhcp ping_packets 4

Success.

DES-3800:admin#
```

config dhcp pool ping_timeout

Purpose	Specifies the amount of time the DHCP server must wait before timing out a ping packet.
Syntax	**config dhcp ping_timeout <milliseconds 10-2000>**
Description	By default, the DHCP server waits 100 milliseconds before timing out a ping packet.
Parameters	*<millisecond 500-2000>* - Amount of time the DHCP server must wait before timing out a ping packet. The default value is 100.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To config the time out value for ping packets:

```
DES-3800:admin# config dhcp ping_timeout 500
Command: config dhcp ping_timeout 500

Success.

DES-3800:admin#
```

create/delete dhcp pool manual_binding

Purpose	Specifies the distinct identification of the client in dotted-hexadecimal notation or harware address, for example, 0122.b708.1388,where 01 represents the Ethernet media type and the IP address pair.
Syntax	**create dhcp pool manual_binding <pool_name 12> < ipaddr> hardware_address <macaddr> {type [ethernet | ieee802]} delete dhcp pool manual_binding <pool_name 12> [<ipaddr> | all]**
Description	An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server. The dynamic binding entry will be created when an IP address is assigned to the client from the pool network's address. For the create dhcp pool manual_binding command, if the type is not specified, the the type will be ethernet . For the match operation, the hardward type and the hardware address field in the protocol fields will be used to match against the entry. The IP address specified in the manual binding entry must be ranged within the network used by the DHCP pool. If the user specifies a conflict IP address, error message will be returned. If a number of manual binding entries are created, and the network address for the pool is changed such that conflict are generated, those manual binding entries which are conflict with the new network address will be automatically deleted.
Parameters	*<pool_name 12>* - Pool's name. *<macaddr>* - Hardware address. *type* - either eithernet or ieee802 can be specified. *<ipaddr>* - IP address which will be assigned to specified client.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To configuring manual bindings:

```
DES-3800:admin#create dhcp pool manual_binding
engineering 10.10.10.1 hardware_address 00-80-C8-02-
02-02 type ethernet
Command: create dhcp pool manual_binding engineering
10.10.10.1 hardware_address 00-80-C8-02-02-02 type
ethernet


Success.


DES-3800:admin#
```

clear dhcp binding

Purpose	This command will delete a binding entry or all binding entries in a pool or clear all binding entries in all pools.
Syntax	**clear dhcp binding [<pool_name 12> [<ipaddr> | all] | all]**
Description	This command clears a binding entry or all binding entries in a pool or clears all binding entries in all pools. Note that this command will not clear the dynamic binding entry which matches a manual binding entry.
Parameters	*<pool_name 12>* - Pool's name. *<ipaddr>* - IP address which will be cleared.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To clear a dynamic binding entries in pool "Engineering".

```
DES-3800:admin#clear dhcp binding Engineering
10.20.3.4
Command: clear dhcp binding Engineering 10.20.3.4

Success.

DES-3800:admin#
```

show dhcp binding

Purpose	Display the current binding entry information.
Syntax	**show dhcp binding {<pool_name 12>}**
Description	This command displays the current binding entry information in a pool or all pools.
Parameters	*<pool_name 12>* - Pool's name.
Restrictions	None.

Usage Example:

To show dynamic binding entries:

```
DES-3800:admin#show dhcp binding engineering
Command: show dhcp binding engineering

Pool Name    IP Address  Hardware address   Type     Status    Lifetime
---------    ----------  ----------------   ----     ------    --------
engineering 192.168.0.1 00-80-C8-08-13-88  Ethernet  Manual    86400
engineering 192.168.0.2 00-80-C8-08-13-99  Ethernet  Automatic 38600

Total Entries : 2

DES-3800:admin#
```

show dhcp pool manual_binding

Purpose	Display the configured manual binding entries.
Syntax	**show dhcp pool manual_binding { pool_name 12}**
Description	This command is used to show manual binding entries. If the pool name is not specified, the information for all pools will be displayed.
Parameters	*<pool_name 12>* - Pool's name.
Restrictions	None.

Usage Example:

To show the configured manual binding entries:

```
DES-3800:admin#show dhcp pool manual_binding
Command: show dhcp pool manual_binding

Pool Name IP Address       Hardware address   Type
--------- --------------   -----------------  ----
p1        192.168.0.1      00-80-C8-08-13-88  Ethernet
p1        192.168.0.2      00-80-C8-08-13-99  Ethernet

Total Entries : 2

DES-3800:admin#
```

show dhcp pool

Purpose	Display the information for dhcp pool.
Syntax	**show dhcp pool {<pool_name>}**
Description	If pool name is not specified, information for all pools will be displayed.
Parameters	*<pool_name 12>* - Pool's name.
Restrictions	None.

Usage Example:

To show the dhcp pool:

```
DES-3800:admin#show dhcp pool engineering
Command: show dhcp pool engineering

Pool Name           : engineering
Network Address     : 10.10.10.0/24
Domain Name         : alpha.com
DNS Server          : 10.10.10.1
NetBIOS Name Server : 10.10.10.1
NetBIOS Node Type   : broadcast
Default Router      : 10.10.10.1
Pool Lease          : 10 days, 0 hours, 0 minutes
Boot File           : boot.bin
Next Server         : 10.10.10.2

DES-3800:admin#
```

enable/disable dhcp_server

Purpose	This command enables or disables the DHCP server function.
Syntax	**enable dhcp_server** **disable dhcp_server**
Description	This command is used to enable or disable the DHCP server function on the Switch. If DHCP relay is enabled, DHCP server can not be enabled. The opposite is also true.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To enable dhcp server.

```
DES-3800:admin#enable dhcp_server
Command: enable dhcp_server

Success.

DES-3800:admin#
```

show dhcp_server

Purpose	This command displays the status of DHCP server.
Syntax	**show dhcp server**
Description	This command will display the current DHCP server on the switch.
Parameters	None.
Restrictions	None.

Usage Example:

To display the dhcp server settings.

```
DES-3800:admin#show dhcp_server
Command: show dhcp_server

DHCP Server  : Disabled
Ping Packets : 2
Ping Timeout : 500 milliseconds

DES-3800:admin#
```

clear dhcp conflict_ip

Purpose	This command clears an entry or all entries from the conflict IP database.
Syntax	**clear dhcp conflict_ip [<ipaddr> | all]**
Description	Clears an address conflict from the DHCP database.
Parameters	*<ip_addr>* - The IP address to be cleared. *all* - All IP addresses will be cleared.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To clear an IP address 10.20.3.4 from the conflict database.

```
DES-3800:admin# clear dhcp conflict_ip 10.20.3.4
Command: clear dhcp conflict_ip 10.20.3.4
Success

DES-3800:admin#
```

show dhcp conflict_ip

Purpose	This command displays the IP address that has been identified as being conflict.
Syntax	**show dhcp conflict_ip {<ipaddr>}**
Description	The DHCP server will use PING packet to determine whether an IP address is in conflict with other host before binding this IP. The IP address which has been identified as a conflict will be moved to the conflict IP database. The system will not attempt to bind the IP address in the conflict IP database unless the user clears it from the conflict IP database.
Parameters	*<ip_addr>* - The IP address to be displayed.
Restrictions	None.

Usage Example:

To display the entries in dhcp conflict_ip database.

```
DES-3800:admin#show dhcp conflict_ip
Command: show dhcp conflict_ip

IP address       Detection Method  Detection time
---------------  ----------------  -------------------
172.16.1.32      Ping              2007/08/30 17:06:59
172.16.1.64      Gratuitous ARP    2007/09/10 19:38:01

Total Entries : 2

DES-3800:admin#
```

60

MLD SNOOPING COMMANDS

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

Command	Parameters
config mld_snooping	[<vlan_name 32> |all] { node_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | done_timer <sec 1-16711450> | state [enable|disable] | fast_done [enable|disable] }
config mld_snooping mrouter_ports	<vlan_name 32> [add|delete]<portlist>
enable mld_snooping	{forward_mcrouter_only}
disable mld_snooping	{forward_mcrouter_only}
show mld_snooping	{vlan <vlan_name 32>}
show mld_snooping group	{vlan <vlan_name 32>}
show mld_snooping forwarding	{vlan <vlan_name 32>}
show mld_snooping mrouter_ports	{vlan <vlan_name 32>} { [static|dynamic]}

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

config mld_snooping

Purpose	Used to configurer MLD snooping on the switch.
Syntax	**config mld_snooping [<vlan_name 32> |all] { node_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | done_timer <sec 1-16711450> | state [enable|disable] | fast_done [enable|disable] }**
Description	The config mld_snooping command configures MLD snooping on the switch.
Parameters	*vlan_name* - The name of the VLAN for which MLD snooping is to be configured. all - Specifies that all VLANs configured on the switch will be configured. *node_timeout* - Specifies the amount of time that must pass before a link node is considered to be not a listener anymore. The default is 260 seconds. *router_timeout* - Specifies the maximum amount of time a router will remain in the switch's can be a listener of a multicast group without the switch receiving a node listener report. The default is 260 seconds. *done_timer* - Specifies the maximum amount of time a group will remain in the switch after receiving a done message of the group without receiving a node listener report. The default setting is 2 seconds. *state* - Allows you to enable or disable the MLD snooping function for the chosen VLAN. *fast_done* - enable or disable MLD snooping fast_done function.If enable, the membership is immediately removed when the system receive the MLD done message.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To configure the MLD snooping to the default vlan with noted_timeout 250 sec and state enable:

```
DES-3800:admin#config mld_snooping default
node_timeout 250 state enable
Command: config mld_snooping default node_timeout 250
state enable

Success.

DES-3800:admin#
```

config mld_snooping mrouter_ports

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

Usage Example:

To set up port range 1-10 to be static router ports:

```
DES-3800:admin#config mld_snooping mrouter_ports
default add 1-10
Command: config mld_snooping mrouter_ports default add
1-10

Success.

DES-3800:admin#
```

enable mld_snooping

Purpose	Used to enable MLD snooping on the switch.
Syntax	**enable mld_snooping {forward_mcrouter_only}**
Description	The enable mld_snooping command allows you to enable MLD snooping on the switch. If forward_mcrouter_only is specified, the switch will forward all multicast traffic to the multicast router, only. Otherwise, the switch forwards all multicast traffic to any IPv6 router.
Parameters	*forward_mcrouter_only* - Specifies that the switch should forward all multicast traffic to a multicast-enabled IPv6 router only. If no parameter is specified, the switch will forward all multicast traffic to any IPv6 router.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To enable MLD snooping on the switch:

```
DES-3800:admin#enable mld_snooping
Command: enable mld_snooping

Success.

DES-3800:admin#
```

disable mld_snooping

Purpose	Used to disable MLD snooping on the switch.
Syntax	**disable mld_snooping**
Description	The disable mld_snooping command disables MLD snooping on the switch. MLD snooping can be disabled only if IPv6 multicast routing is not being used. Disabling MLD snooping allows all MLD and IPv6 multicast traffic to flood within a given IPv6 interface.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Usage Example:

To disable MLD snooping on the switch:

```
DES-3800:admin#disable mld_snooping
Command: disable mld_snooping

Success.

DES-3800:admin#
```

show mld_snooping

Purpose	Used to show the current status of MLD snooping on the switch.
Syntax	**show mld_snooping {vlan <vlan_name 32> }**
Description	The show mld_snooping will display the current MLD snooping configuration on the switch.
Parameters	*vlan_name* - The name of the VLAN for which you want to view the MLD snooping configuration. If no parameter specified, the system will display all current MLD snooping configuration.
Restrictions	None.

Usage Example:

To show MLD snooping on the switch:

```
DES-3800:admin#show mld_snooping
Command: show mld_snooping

MLD Snooping Global State    : Disabled
Multicast router Only        : Disabled

VLAN  Name                   : default
Max Response Time            : 10
Robustness Value             : 2
Node Timeout                 : 260
Router Timeout               : 260
Done Timer                   : 2
Querier State                : Disabled
Querier Router Behavior      : Non-Querier
State                        : Disabled

VLAN  Name                   : vlan2
```

show mld_snooping group

Purpose	Used to display the current MLD snooping group configuration on the switch.
Syntax	**show mld_snooping group {vlan <vlan_name 32>}**
Description	The show mld_snooping group displays the current MLD snooping group configuration on the switch.
Parameters	*vlan_name* - The name of the VLAN for which you want to view the MLD snooping configuration. If no parameter specified, the system will display all current MLD snooping configuration.
Restrictions	None.

Example:

To show MLD Snooping group on the switch:

```
DES-3800:admin#show mld_snooping group
Command: show mld_snooping group

VLAN Name         : default
Multicast group   : FF02::13
MAC address       : 33-33-00-00-00-13
Reports           : 1
Port Listener     : 1,7

VLAN Name         : default
Multicast group   : FF02::14
MAC address       : 33-33-00-00-00-14
Reports           : 1
Port Listener     : 2,7

VLAN Name         : default
Multicast group   : FF02::15
MAC address       : 33-33-00-00-00-15
Reports           : 1
Port Listener     : 2,9

VLAN Name         : default
Multicast group   : FF02::16
MAC address       : 33-33-00-00-00-16
Reports           : 1
Port Listener     : 2,7

VLAN Name         : default
Multicast group   : FF02::17
MAC address       : 33-33-00-00-00-17
Reports           : 2
Port Listener     : 2,7

VLAN Name         : default
Multicast group   : FF02::18
MAC address       : 33-33-00-00-00-18
Reports           : 1
Port Listener     : 1,7

Total Entries : 6

DES-3800:admin#
```

show mld_snooping forwarding

Purpose	Used to display the current MLD snooping forwarding table of the switch.
Syntax	**show mld_snooping forwarding {vlan <vlan_name 32>}**
Description	The show mld_snooping forwarding command displays the current MLD snooping forwarding table of the switch.
Parameters	*vlan_name* - The name of the VLAN for which you want to view the MLD snooping configuration. If no parameter specified, the system will display all current MLD snooping configuration.
Restrictions	None.

Usage Example:

To show all MLD snooping entries on the switch:

```
DES-3800:admin#show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name      : default
Source IP      : FE08::C
Multicast Group: FF02::17
Listening Port   : 7

VLAN Name      : default
Source IP      : FE08::d
Multicast Group: FF02::23
Listening Port   : 3

VLAN Name      : default
Source IP      : FE08::e
Multicast Group: FF02::35
Listening Port   : 10

Total Entries : 3

DES-3800:admin#
```

show mld_snooping mrouter_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	**show mld_snooping mrouter_ports {vlan <vlan_name 32>}{static|dynamic}**
Description	The show mld_snooping mrouter_ports command displays the currently configured router ports on the switch.
Parameters	*vlan_name* - The name of the VLAN on which the router port resides. *static* - Displays router ports that have been statically configured. *dynamic* - Displays router ports that have been dynamically configured. *forbidden* - Displays forbidden router ports that have been statically configured. If no parameter specified, the system will display all currently configured router ports on the switch.
Restrictions	None.

Usage Example:

To display the router ports:

```
DES-3800:admin#show mld_snooping mrouter_ports
Command: show mld_snooping mrouter_ports

VLAN Name               : default
Static mrouter port     : 1-10
Dynamic mrouter port    :
Forbidden mrouter port  :

VLAN Name               : vlan2
Static mrouter port     :
Dynamic mrouter port    :
Forbidden mrouter port  :

Total Entries : 2

DES-3800:admin#
```

61

LOOPBACK DETECTION COMMANDS

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

Command	Parameters
config loopdetect	{recover_timer [0 | <value 60-1000000>] | interval <1-32767> | mode [port-based | vlan-based]] (1)
config loopdetect ports	[<portlist>| all] state [enable | disable]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[all | <portlist>]

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

config loopdetect

Purpose	Used to configure loop-back detection function on the switch.
Syntax	**config loopdetect {recover_timer [0 | <value 60-1000000>] | interval <1-32767> | mode [port-based | vlan-based]} (1)**
Description	The config loopdetect command is used to setup the loop-back detection function (LBD) for the entire switch.
Parameters	*recover_timer* - The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. The valid range is 60 to 1000000 . Zero is a special value which means to disable the auto-recovery mechanism, hence, user need to recover the disabled port back manually. Default value of recover_timer is 60. *interval* - The time interval (in seconds) at which device transmits all the CTP(Configuration Test Protocol) packets to detect the loop-back event. The default setting is 10. Valid range is 1 to 32767. *mode* - Choose the loop-detection operation mode. In the port-based mode , the port will be shut-down (disabled) when detecting loop ; in vlan-based mode , the port can’t process packets of the VLAN that detecting the loop.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To set recover_time 0 , interval 20 mode vlan-based:

```
DES-3800:admin# config loopdetect  recover_timer 0
interval 20 vlan-based
Command: config loopdetect  recover_timer 0 interval
20 vlan-based

Success.

DES-3800:admin#
```

config loopdetect ports

Purpose	Used to configure loop-back detection function for the port on the switch.
Syntax	**config loopdetect ports [<portlist>| all] state [enable | disable]**
Description	The config loopdetect port command is used to setup the loop-back detection function for the interface on the switch.
Parameters	*portlist* - Specifies a range of ports to be configured. *all* - For set all ports in the system , you may use “all” parameter. *state* - Allows loop-detect to be enabled or disabled for the ports specified in the port list. The default is disabled.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To set state enable:

```
DES-3800:admin# config loopdetect ports 1-5 state
enable
Command: config loopdetect ports 1-5 state enable

Success.

DES-3800:admin#
```

enable loopdetect

Purpose	Used to globally enable loopdetect function on the switch.
Syntax	**enable loopdetect**
Description	The enable loopdetect command allows the Loop Detection Function to be globally enabled on the switch. The default value is disabled.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the loopdetect:

```
DES-3800:admin#enable loopdetect
Command: enable loopdetect

Success.

DES-3800:admin#
```

disable loopdetect

Purpose	Used to globally disable loopdetect function on the switch.
Syntax	**disable loopdetect**
Description	The disable loopdetect command allows the Loop Detection Function to be globally disabled on the switch. The default value is disabled.
Parameters	None.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To enable the loopdetect:

```
DES-3800:admin#disable loopdetect
Command: disable loopdetect

Success.

DES-3800:admin#
```

show loopdetect

Purpose	Used to display the switch's current loopdetect configuration.
Syntax	**show loopdetect**
Description	The show loopdetect command displays the switch's current loopdetect configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the current loopdetect configuration:

```
DES-3800:admin#show loopdetect
Command: show loopdetect
Loopdetect Global Settings
---------------------------------
Loopdetect Status        : Enabled
Loopdetect Interval      : 20
Recover Time             : 60
Mode                     : VLAN-Based

DES-3800:admin#
```

show loopdetect ports

Purpose	Used to display the switch's current per-port loopdetect configuration.
Syntax	**show loopdetect ports [all | <portlist>]**
Description	The show loopdetect ports command displays the switch's current per-port loopdetect configuration and status.
Parameters	*portlist* - Specifies a range of ports to be displayed. all - System will display all ports loopdetect information.
Restrictions	None.

Example usage:

To display loopdetect state of port 1-9 under port-based mode:

```
Command: show loopdetect  ports 1-9

Port   Loopdetect State   Loop Status
------ ------------------ ----------
1      Enabled            Normal
2      Enabled            Normal
3      Enabled            Normal
4      Enabled            Normal
5      Enabled            Loop!
6      Enabled            Normal
7      Enabled            Loop!
8      Enabled            Normal
9      Enabled            Normal

DES-3800:admin#
```

To display loopdetect state of port 1-9 under vlan-based mode：

```
DES-3800:admin#show loopdetect  ports 1-9
Command: show loopdetect  ports 1-9

Port   Loopdetect State    Loop VLAN
------ ------------------ ----------
1      Enabled            None
2      Enabled            None
3      Enabled            None
4      Enabled            None
5      Enabled            2
6      Enabled            None
7      Enabled            2
8      Enabled            None
9      Enabled            None

DES-3800:admin#
```

62

PASSWORD RECOVERY COMMANDS

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

Command	Parameters
reset password <username>	
reset factory	
restart	
reset account {<username>}	
show account_list	

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

reset password	
Purpose	Used to reset (set to empty) already created account's password
Syntax	*reset password <username>*
Description	The reset password command reset (set to empty) already created account's password.
Parameters	*username* - To specify the user name for the account to be reset.
Restrictions	This command is only available in password recovery mode.

Example usage:

To reset the password:

```
>reset password user1
Command: reset password user1

Success.

>
```

reset factory	
Purpose	Used to reset the configuration to default setting.
Syntax	**reset factory**
Description	The reset factory command reset to default setting.
Parameters	None.
Restrictions	This command is only available in password recovery mode.

Example usage:

To reset the factory defaults:

```
>reset factory
Command: reset factory

Success.

>
```

restart

Purpose	Used to exit Reset Configuration Mode and restart the switch.
Syntax	**restart**
Description	The restart command exit Reset Configuration Mode and restart the switch. If the configuration had been modified, it pops out a confirmation message to save the current setting.
Parameters	None.
Restrictions	This command is only available in password recovery mode.

Example usage:

To restart the Switch:

```
>restart
Command: restart

Are you sure to proceed with the system reboot?(y/n)
Are you want to save configuration?(y/n)
Saving all configurations to NV-RAM..... Done.
Please wait, the switch is rebooting...
```

reset account

Purpose	Used to delete the created account.
Syntax	**reset account {<username>}**
Description	The reset account command deletes the created account. If the user doesn’t specify the username, all accounts will be deleted.
Parameters	username - The user to be reset.
Restrictions	This command is only available in password recovery mode.

Example usage:

To reset an account:

```
>reset account
Command: reset account

Success
```

show account_list

Purpose	Used to show the created account.
Syntax	**show account_list**
Description	The show account_list command display all already created accounts.
Parameters	None.
Restrictions	This command is only available in password recovery mode.

Example usage:

To display the account list:

```
Command: show account_list

Current Accounts:
Username         Access Level
--------------   ------------
admin1           Admin
user1            User

Total Entries : 2

>
```

63

MULTICAST VLAN COMMANDS

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

Command	Parameters
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 32> {member_port <portlist> | source_port <portlist> | state [enable | disable] {force_agree} }
delete igmp_snooping multicat_vlan	<vlan_name 32>
show igmp_snooping multicast_vlan	{<vlan_name 32>}

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

create igmp_snooping multicast_vlan

Purpose	Used to create a multicast VLAN.
Syntax	**create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>.**
Description	The create igmp_snooping multicast_vlan command will create a multicast_vlan. Multiple multicast VLAN can be configured.
Parameters	*vlan_name* - The name of the multicast VLAN to be created, Each multicast VLAN is given a name that can be up to 32 characters. *vlanid* - The VLAN ID of the multicast VLAN to be created. The range is 2 - 4094.
Restrictions	Only Administrator or Operator-level users can issue this command. The ISM VLAN being created can not exist in the 1Q VLAN database. Multiple ISM VLAN can be created. The ISM VLAN snooping function co-exist with the 1Q VLAN snooping function.

Example usage:

To create igmp_snoop multicast_vlan mv1 2:

```
DES-3800:admin# create igmp_snoop multicast_vlan mv1
2
Command: create igmp_snoop multicast_vlan mv1 2

Success.

DES-3800:admin#
```

config igmp_snooping multicast_vlan

Purpose	Used to configure the parameter of the specific multicast VLAN.
Syntax	**config igmp_snooping multicast_vlan <vlan_name 32> {member_port <portlist> | source_port <portlist> | state [enable | disable] {force_agree} }**
Description	The config igmp_snooping multicast_vlan command allows you to update member portlist and update source portlist. The member port are the untagged member of the multicast VLAN, and the source port will automatically become the tagged member of the multicast VLAN. To change the port-list, the new port-list will replace the previous port-list.
Parameters	*vlan_name* - The name of the multicast VLAN to be configured, Each multicast VLAN is given a name that can be up to 32 characters. *member_port* - A range of member ports to add to the multicast VLAN. They will become the untagged member port of the ISM VLAN. *source_port* - A range of member ports to add to the multicast VLAN. *state* - enable or disable multicast VLAN for the chosen VLAN. *force_agree* - When force_agree is specified, the config command will be executed immediatedly without further confirmation.
Restrictions	The member port list and source port list could not overlap. The multicast vlan must be created first before configuration. Only Administrator or Operator-level users can issue this command.

Example usage:

To config igmp_snoop multicast_vlan:

```
DES-3800:admin# config igmp_snooping multicast_vlan
v1 member_port 1,3 source_port 2
state enable
Command: config igmp_snooping multicast_vlan v1
member_port 1,3 source_port 2
state enable


Success.


DES-3800:admin#
```

delete igmp_snooping multicast_vlan

Purpose	Used to delete a muticast VLAN.
Syntax	**delete igmp_snooping multicat_vlan <vlan_name 32>**
Description	The delete igmp_snooping multicast_vlan command allows you to delete multicat_vlan.
Parameters	*vlan_name* - The name of the multicast VLAN to be deleted.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To delete igmp_snoop multicast_vlan:

```
DES-3800:admin# delete igmp_snooping multicat_vlan
v1
Command: delete igmp_snooping multicat_vlan v1

Success.

DES-3800:admin#
```

show igmp_snooping multicast_vlan

Purpose	Used to show the information of multicast VLAN.
Syntax	**show igmp_snooping multicast_vlan {<vlan_name 32>}**
Description	The show igmp_snooping multicast_vlan command allows you to show the information of multicat_vlan.
Parameters	*vlan_name* - The name of the multicast VLAN to be shown.
Restrictions	None.

Example usage:

To show igmp_snoop multicast_vlan:

```
DES-3800:admin# show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

VLAN Name              :mv1
VID                    : 2
Member          Ports  : 1,3
Source Ports           : 4
Status                 : Enabled

DES-3800:admin#
```

64

CPU FILTERING COMMANDS LIST

The CPU Filtering Commands List is used to display and configure the l3 control packets sent to the CPU from specific ports.

Command	Parameters
config cpu_filter l3_control_pkt	<portlist> [dvmrp | pim | igmp_query | ospf | rip |vrrp | all] state [enable | disable]
show cpu_filter l3_control_pkt	{<portlist>}

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

config cpu_filter l3_control_pkt

Purpose	This command is used to discard the l3 control packets sent to the CPU from specific ports.
Syntax	**config cpu_filter l3_control_pkt <portlist> [dvmrp | pim | igmp_query | ospf | rip |vrrp | all] state [enable | disable]**
Description	This command is used to discard the l3 control packets sent to CPU from specific ports.
Parameters	*<portlist>*- Specify the port list to filter control packet *dvmrp*- Specify to filter the DVMRP protocol. *pim*- Specify to filter the PIM protocol. *igmp_query*- Specify to filter the IGMP Query protocol. *ospf*- Specify to filter the OSPF protocol. *rip*- Specify to filter the RIP protocol. *vrrp*- Specify to filter the VRRP protocol. *all*- Specify to filter All the l3 control packets. *state*- Enable or disable the filtering function. Default is disabled
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To filter DVMRP and OSPF on ports 1-26:

```
DES-3800:admin# config filter control_packet 1-26
dvmrp ospf state enable
Command: config filter control_packet 1-26 dvmrp
ospf state enable
Success.

DES-3800:admin#
```

show cpu_filter l3_control_pkt

Purpose	Used to display the l3 control packet CPU filtering status.
Syntax	**show cpu_filter l3_control_pkt {<portlist>}**
Description	Used to display the l3 control packet CPU filtering status.
Parameters	*<portlist>*- Specify the list of ports that need to filter control packets.
Restrictions	None.

Example usage:

To display the filtering status for ports 1 and 2:

```
DES-3800:admin#show cpu_filter l3 control_pkt 1-2
Command: show cpu_filter l3 control_pkt 1-2

Port  RIP       OSPF      VRRP      PIM      DVMRP      IGMP Query
----  --------  --------  --------  --------  --------  -----------
1     Disabled  Enabled   Disabled  Disabled  Enabled   Disabled
2     Enabled   Enabled   Disabled  Disabled  Disabled  Disabled

DES-3800:admin#
```

65

BROADCAST SEGMENTATION COMMANDS

The Broadcast Segmentation Commands can be used to isolate some kind of traffic, such as broadcast or l2 unknown multicast traffic. Broadcast Segmentation can isolate layer 2 broadcast domains between ports, while keeping IP traffic forwarded between ports. This feature is particularly useful in an Ethernet-to-the-Home environment where broadcasts need to be blocked between each house-hold, while allowing IP communication between them. This method of segmenting the flow of traffic is similar to cross-VLAN routing, but can save the number of IP addresses used for configuring IP interfaces/subnets per VLAN.

Command	Parameters
config broadcast_filter	[<portlist> | all | null] {arp_forward_list [<portlist> | all | null]}
show broadcast_filter	

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

config broadcast_filter	
Purpose	The broadcast filter is used to isolate some kind of traffic, such as broadcast or l2 unknown multicast traffic.
Syntax	**config broadcast_filter [<portlist> | all | null] { arp_forward_list [<portlist> | all | null] }**
Description	The command isolates broadcast or l2 unknown multicast traffic,but allows the user to set forward ARP requests by port.
Parameters	*broadcast_filter*- When a port is listed in the <portlist>, the broadcast, unknown multicast from other ports to this port will be dropped; the broadcast, unknown multicast from this port to other non-listed ports will still be forwarded. *<portlist>*- Specifes a range of ports to be configured. *all*- Specifies that all ports are to be configured. *null*- Specifies that the range of the port filter domain is null. *arp_forward_list*- Specifies a range of ports that need to forward ARP requests. When a port is listed, the ARP packets, which are broadcast packets, from other ports to this port will be forwarded. *<portlist>*-Specifes a range of ports to be configured. *all*- Specifes that all of ports are be configured. *null*- Specifies that the range of the port filter domain is null.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To config a broadcast filter:

```
DES-3800:admin#config broadcast_filter 1-5
arp_forward_list 1-5
Command: config broadcast_filter 1-5
arp_forward_list 1-5


Success.
```

show broadcast_filter

Purpose	Displays the portlist of forbidden broadcast traffic.
Syntax	**show broadcast_filter**
Description	The command displays the portlist of forbidden broadcast traffic.
Parameters	None.
Restrictions	None.

Example usage:

To display the broadcast filter :

```
DES-3800:admin#show broadcast_filter
Command: show broadcast_filter

Port         Filter State           ARP Forward State
----         -------------          -----------------
1             Filter                 Forward
2             Filter                 Forward
3             Filter                 Forward
4             Filter                 Forward
5             Filter                 Forward
6             Forward                Not Forward
7             Forward                Not Forward
8             Forward                Not Forward
9             Forward                Not Forward
10            Forward                Not Forward
11            Forward                Not Forward
12            Forward                Not Forward
13            Forward                Not Forward
14            Forward                Not Forward
15            Forward                Not Forward
16            Forward                Not Forward
```

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 802.1 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 IEEE 802.3af Power over Ethernet	
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-3828/DES-3852 AC Input: 100 – 120; 200 – 240 VAC, 50/60 Hz DES-3828P AC Input: 100 – 120; 200 – 240 VAC, 50/60 Hz PoE: Output capacity for whole system: 370W Per Port: 15.4W (Default) Per port → 1~16.8W (Can be set) DES-3828 DC DC Power Input: 48 V
Power Consumption	DES-3828/DES-3828DC/DES-3852: 24 watts maximum DES-3828P: 395.2 watts maximum
DC fans:	DES-3828/DES-3828DC/DES-3828P/DES-3852: one 15cm fan DES-3852: two 8.3cm fans DES-3828P: one additional 270mm blower
Operating Temperature	0 - 40°C
Storage Temperature	-40 - 70°C
Humidity	5 - 95% non-condensing
Dimensions	DES-3828/DES3828DC/DES-3852: 441 mm x 310 mm x 44 mm DES-3828P: 441mm x 369mm x 44mm
Weight	DES-3828/DES-3828DC: 4.24kg (9.35lbs) DES-3852: 4.25kg (9.38lbs) DES-3828P: 6.02kg (13.27lbs)
EMI:	CE class A, FCC Class A, VCCI Class A, C-Tick
Safety:	CSA International, CB Report

Performance	
Transmission Method	Store-and-forward
Packet Buffer	32 MB per device
Packet Filtering / Forwarding Rate	14,881 pps (10M port) 148.810 pps (100M port) 1,488,100 pps (1Gbps port)
MAC Address Learning	Automatic update. Supports 16K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.

Appendix B

ARP Packet Content ACL

Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address (MAC address) when only its IP address is known. This protocol is vulnerable that crackers can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce ARP protocol, ARP spoofing attacks, and the countermeasure brought by D-Link's switches to throttle the ARP spoofing attack.

How Address Resolution Protocol works

In the process of ARP, PC A will, firstly, issue an ARP request to query PC B's MAC address. The network structure is shown in Figure-1.

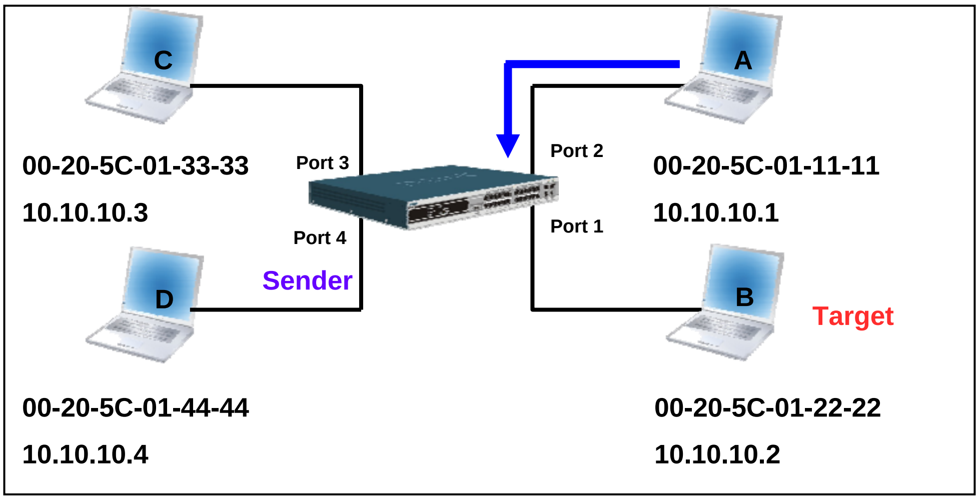


Figure-1

At the mean time, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00" while PC B's IP address will be written into the "Target Protocol Address", shown in Table-1.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP request	**00-20-5C-01-11-11**	**10.10.10.1**	**00-00-00-00-00-00**	**10.10.10.2**

Table -1 (ARP Payload)

The ARP request will be encapsulated into Ethernet frame and sent out. As can be seen in Table-2, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since ARP request is sent via broadcast, the "Destination address" is in a format of Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Table-2 (Ethernet frame format)

Destination address	Source address	Ether-type	ARP	FCS
FF-FF-FF-FF-FF-FF	**00-20-5C-01-11-11**			

When the switch receives the frame, it will check the "Source Address" in the Ethernet frame's header. If the address is not in its Forwarding Table, the switch will learn PC A's MAC and the associated port into its Forwarding Table.

Forwarding Table	
Port1	00-20-5C-01-11-11

In addition, when the switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure -2).

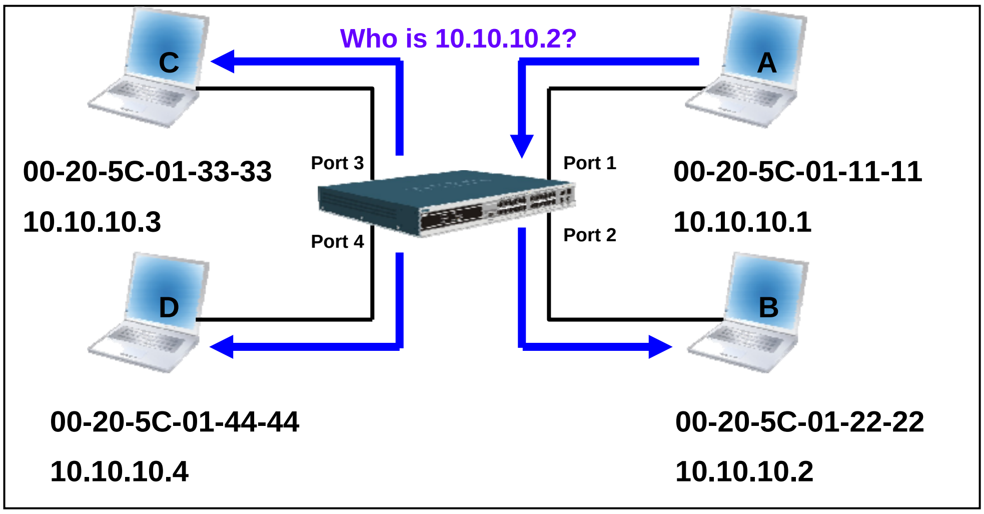


Figure - 2

When the switch floods the frame of ARP request to the network, all PCs will receive and examine the frame but only PC B will reply the query as the destination IP matched (see Figure-3).

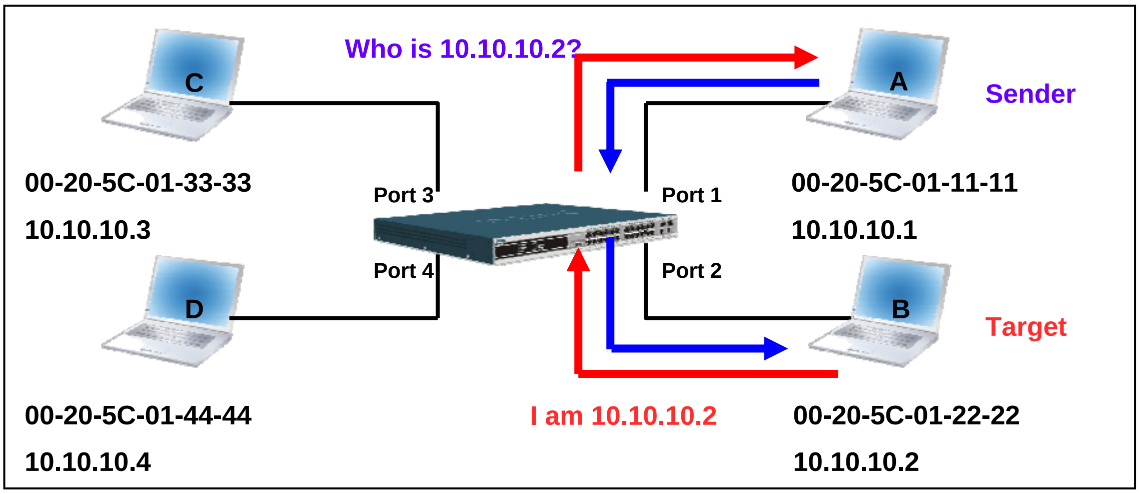


Figure-3

When PC B replies the ARP request, its MAC address will be written into "Target H/W Address" in the ARP payload shown in Table-3. The ARP reply will be then encapsulated into Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP reply	***00-20-5C-01-11-11***	***10.10.10.1***	***00-20-5C-01-22-22***	***10.10.10.2***

Table – 3 (ARP Payload)

When PC B replies the query, the "Destination Address" in the Ethernet frame will be changed to PC A's MAC address. The "Source Address" will be changed to PC B's MAC address (see Table-4).

Destination address	Source address	Ether-type	ARP	FCS
00-20-5C-01-11-11	***00-20-5C-01-22-22***			

Table – 4 (Ethernet frame format)

The switch will also examine the "Source Address" of Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B's MAC and update its Forwarding Table.

Forwarding Table

Port1	**00-20-5C-01-11-11**
Port2	**00-20-5C-01-22-22**

How ARP spoofing attacks a network

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service - DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC addresses with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

IP spoofing attacks are caused by Gratuitous ARPs that occur when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

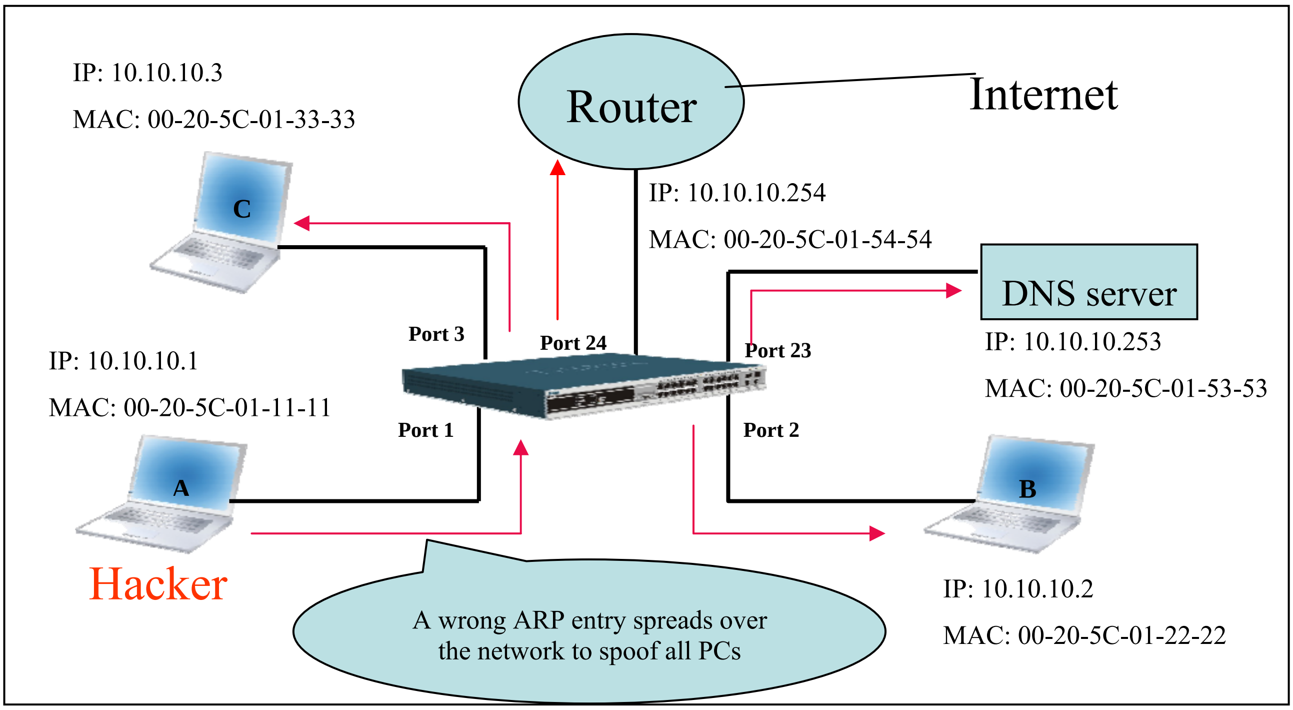


Figure-4

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address itself. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of Gratuitous ARP is shown in Table-5.

Ethernet Header			Gratuitous ARP								
Destination address	Source address	Ethernet type	H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	806					**ARP reply**	**00-20-5C-01-11-11**	**10.10.10.254**	**00-20-5C-01-11-11**	**10.10.10.254**

Table-5

A common DoS attack today can be done by associating a nonexistent or any specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast ONE Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets sent through the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker fools the victims PC to make it believe it is a router and fools the router to make it believe it is the victim. As can be seen in Figure-5 all traffic will be then sniffed by the hacker without the users knowledge.

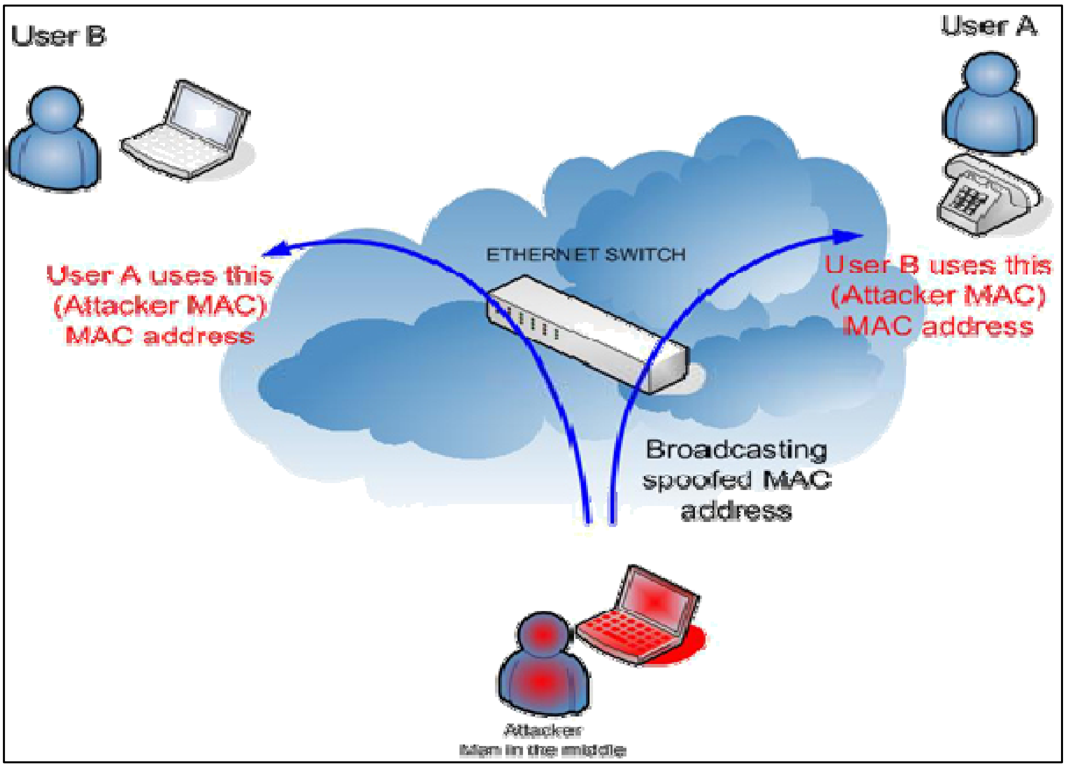
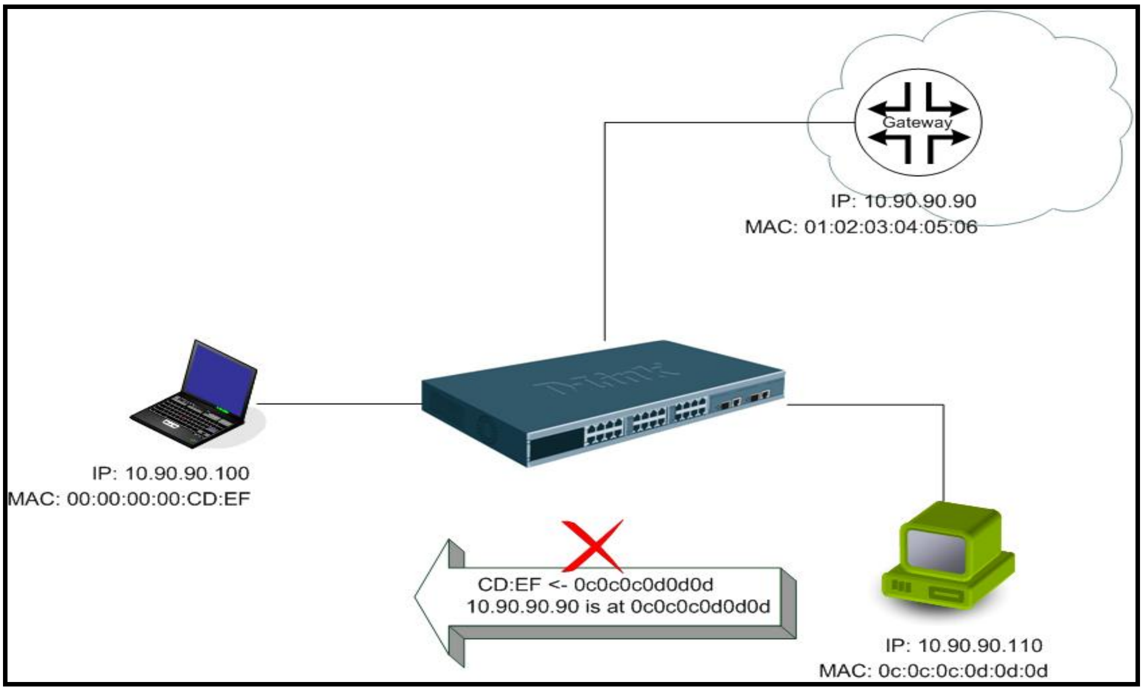

User B
User A
User A uses this (Attacker MAC) MAC address
ETHERNET SWITCH
User B uses this (Attacker MAC) MAC address
Broadcasting spoofed MAC address
Attacker
Man in the middle

Figure-5

Prevent ARP spoofing via packet content ACL

Concerning the common DoS attack today caused by the ARP spoofing, D-Link managed switch can effectively mitigate it via its unique Packet Content ACL.

For the reason that basic ACL can only filter ARP packets based on packet type, VLAN ID, Source and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attacks, we will demonstrate here using the Packet Content ACL on the DES-3800 to block the invalid ARP packets which contain faked gateway's MAC and IP binding.



Example Topology

Configuration:

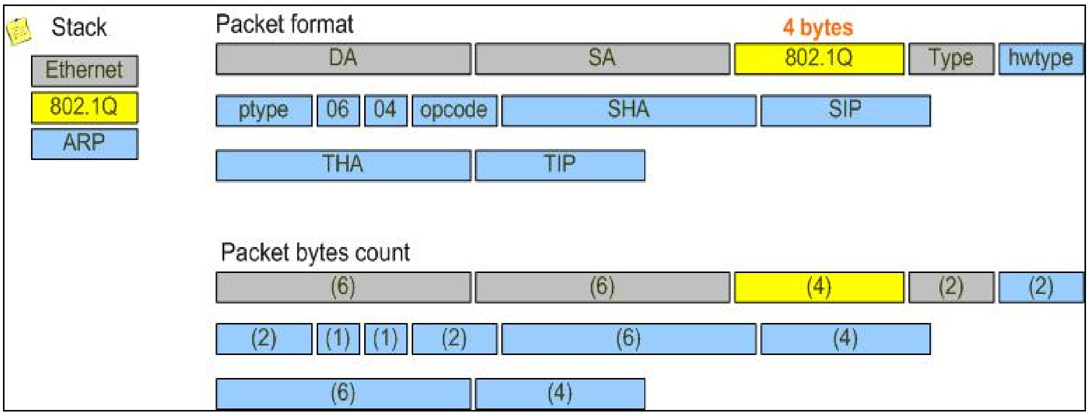
The design of the Packet Content ACL on the DES-3800 series can inspect any specified content in the first 48 bytes of an ARP packet (up to 80 bytes in total at one time). It utilizes offsets to match individual fields in the Ethernet Frame. An offset contains 16 bytes and each offset is divided into four 4-byte values in a HEX format. (refer to the configuration example below for details)

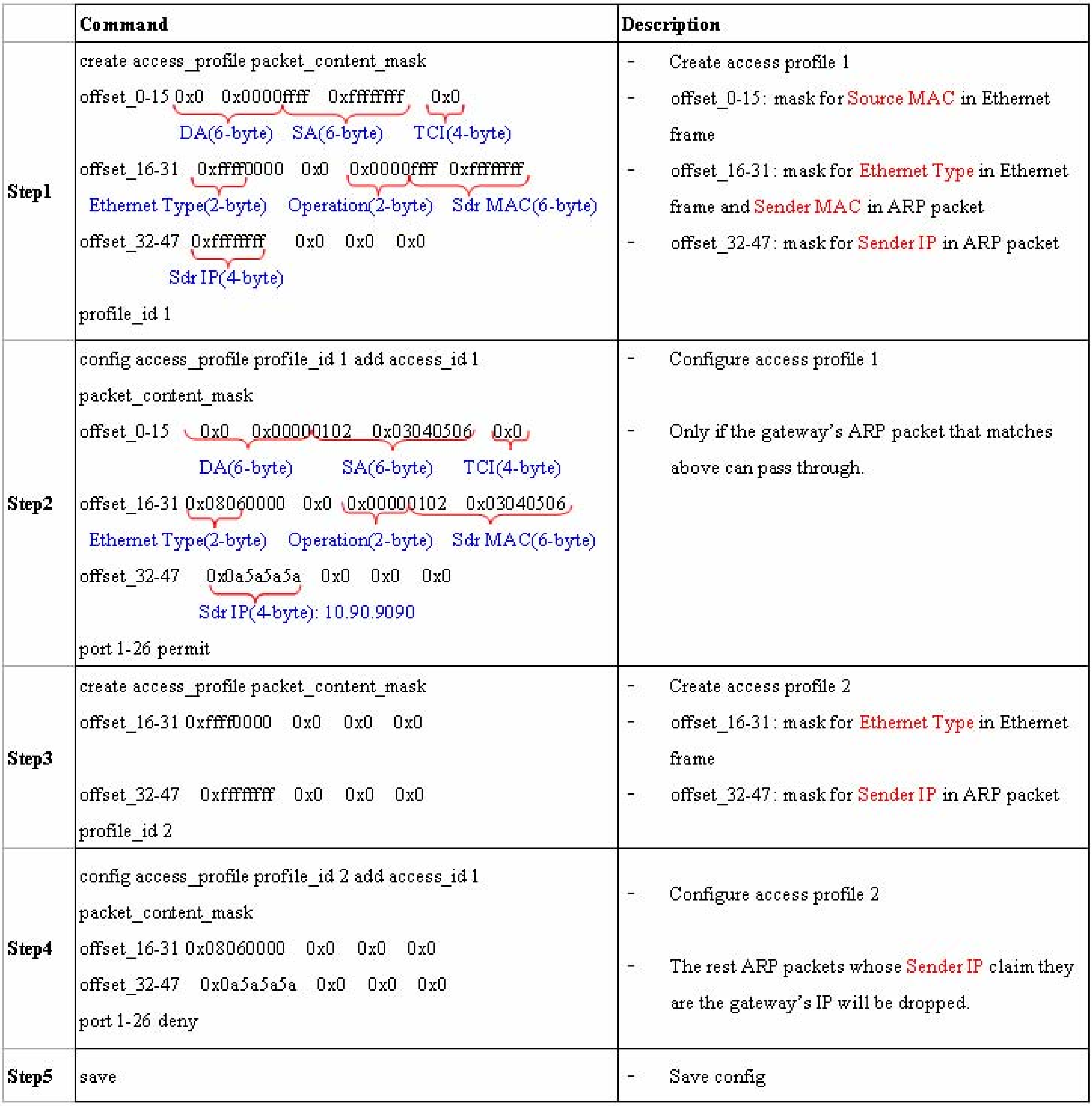
In addition, the configuration logics are:

1. Only if the ARP matches the Source MAC addresses in Ethernet, Sender's MAC address and Senders IP address in the ARP protocol can it pass through the switch. (In this example, it is gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

When calculating packet offset on DES-3800 series, remember that even though a port is an untagged port, the packet will add additional **4 bytes** of 802.1Q header (TCI) for switching internal process, shown in Figure-6.

All packets will be added additional 4 bytes to assign PVID for switching internal process.


Stack
Ethernet
802.1Q
ARP
Packet format
4 bytes
DA
SA
802.1Q
Type
hwtype
ptype
06
04
opcode
SHA
SIP
THA
TIP
Packet bytes count
(6)
(6)
(4)
(2)
(2)
(2)
(1)
(1)
(2)
(6)
(4)
(6)
(4)



	Command	Description
Step1	create access_profile packet_content_mask offset_0-15 0x0 0x0000ffff 0xffffffff 0x0 DA(6-byte) SA(6-byte) TCI(4-byte) offset_16-31 0xffff0000 0x0 0x0000ffff 0xffffffff Ethernet Type(2-byte) Operation(2-byte) Sdr MAC(6-byte) offset_32-47 0xffffffff 0x0 0x0 0x0 Sdr IP(4-byte) profile_id 1	- Create access profile 1 - offset_0-15 : mask for Source MAC in Ethernet frame - offset_16-31 : mask for Ethernet Type in Ethernet frame and Sender MAC in ARP packet - offset_32-47 : mask for Sender IP in ARP packet
Step2	config access_profile profile_id 1 add access_id 1 packet_content_mask offset_0-15 0x0 0x00000102 0x03040506 0x0 DA(6-byte) SA(6-byte) TCI(4-byte) offset_16-31 0x08060000 0x0 0x00000102 0x03040506 Ethernet Type(2-byte) Operation(2-byte) Sdr MAC(6-byte) offset_32-47 0x0a5a5a5a 0x0 0x0 0x0 Sdr IP(4-byte): 10.90.9090 port 1-26 permit	- Configure access profile 1 - Only if the gateway's ARP packet that matches above can pass through.
Step3	create access_profile packet_content_mask offset_16-31 0xffff0000 0x0 0x0 0x0 offset_32-47 0xffffffff 0x0 0x0 0x0 profile_id 2	- Create access profile 2 - offset_16-31 : mask for Ethernet Type in Ethernet frame - offset_32-47 : mask for Sender IP in ARP packet
Step4	config access_profile profile_id 2 add access_id 1 packet_content_mask offset_16-31 0x08060000 0x0 0x0 0x0 offset_32-47 0x0a5a5a5a 0x0 0x0 0x0 port 1-26 deny	- Configure access profile 2 - The rest ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step5	save	- Save config