CLI Reference Guide

Product Model: DES-1210-52/ME

L2 Managed Metro Ethernet Switch

Version 1.00 (release 20.01)

Information in this document is subject to change without notice.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at hisown expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Sept, 2014

Table of Contents

1

INTRODUCTION

The DES-1210-52/ME is L2 Metro Ethernet switche. It consists of 48 10/100Mbps ports plus 4 combo 10/100/1000Base-T ports and 2 dedicated SFP ports.

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. For detailed information on installing hardware please refer also to the Manual.

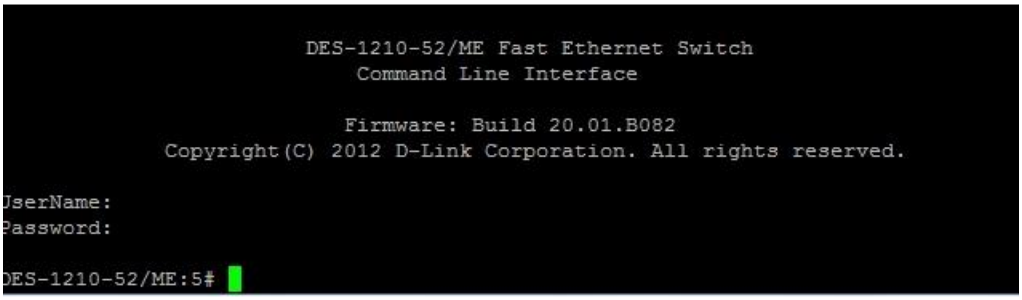
Accessing the Switch via the Serial Port.

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

- 9600 bps
- 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 then connected to the Switch's serial port via an RJ-45 cable.

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



```
                     DES-1210-52/ME Fast Ethernet Switch
                         Command Line Interface

                        Firmware: Build 20.01.B082
            Copyright(C) 2012 D-Link Corporation. All rights reserved.

JserName:
Password:

DES-1210-52/ME:5#
```

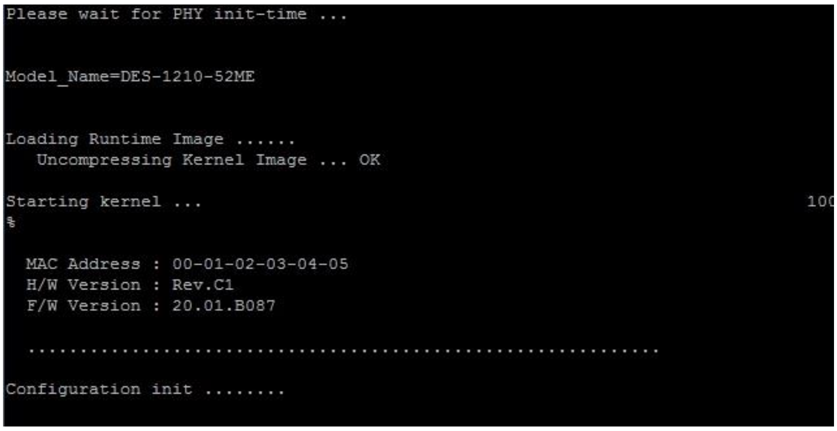
Figure 1–1 Initial CLI screen

There is no initial username or password. Just press the Enter key twice to display the CLI input cursor − DES-1210-52/ME:5#. 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, but can be found on the initial boot console screen – shown below.



```
Please wait for PHY init-time ...


Model_Name=DES-1210-52ME


Loading Runtime Image ......
   Uncompressing Kernel Image ... OK

Starting kernel ...                                                    10
%

  MAC Address : 00-01-02-03-04-05
  H/W Version : Rev.C1
  F/W Version : 20.01.B087

  ..........................................................

Configuration init ........
```

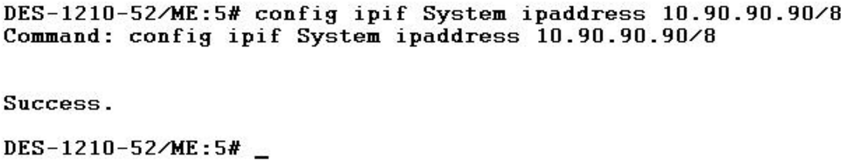
Figure 1–2 Boot Screen

The Switch's MAC address can also be found in the Web management program on the Switch Information (Basic Settings) window in the Configuration folder.
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:
Starting at the command line prompt, enter the command 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.

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

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



```
DES-1210-52/ME:5# config ipif System ipaddress 10.90.90.90/8
Command: config ipif System ipaddress 10.90.90.90/8


Success.

DES-1210-52/ME:5# _
```

Figure 1–3 Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.90.90.91 with a subnet mask of 255.0.0.0. The system message Success. indicates that the command was executed Success.fully. 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 a 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 is loaded.

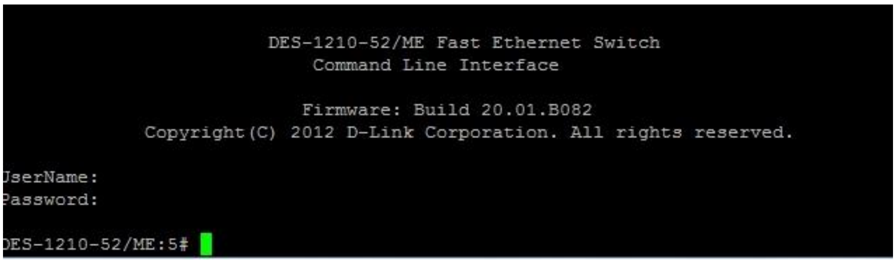
Connecting to the Switch

The console interface is used by connecting the Switch to a VT100-compatible terminal or a computer running an ordinary terminal emulator program (for example, the HyperTerminal program included with the Windows operating system) using an RJ-45 serial cable. Your terminal parameters will need to be set to:

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

The same functions may also be accessed over a Telnet interface. Once an IP address for the Switch has been set, A Telnet program can be used (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 to logged in, the console looks like this:

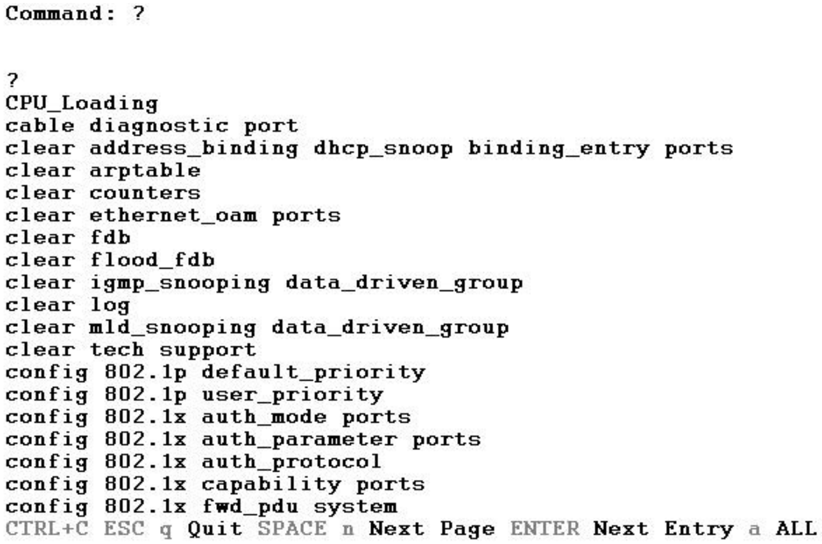


```
                    DES-1210-52/ME Fast Ethernet Switch
                        Command Line Interface

                       Firmware: Build 20.01.B082
          Copyright(C) 2012 D-Link Corporation. All rights reserved.

UserName:
Password:

DES-1210-52/ME:5#
```

Figure 2–1 Initial Console Screen after Logging In

Commands are entered at the command prompt, DES-1210-52/ME:5#

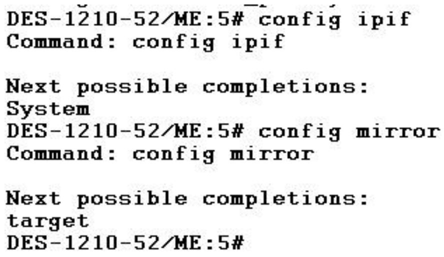
There are a number of helpful features included in the CLI. Entering the ? command displays a list of all of the top-level commands.



```
Command: ?


?
CPU_Loading
cable diagnostic port
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear ethernet_oam ports
clear fdb
clear flood_fdb
clear igmp_snooping data_driven_group
clear log
clear mld_snooping data_driven_group
clear tech support
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode ports
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x fwd_pdu system
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

Figure 2–2 The ? Command

When entering a command without its required parameters, the CLI displays the prompt: command: config account message and the options listed below.



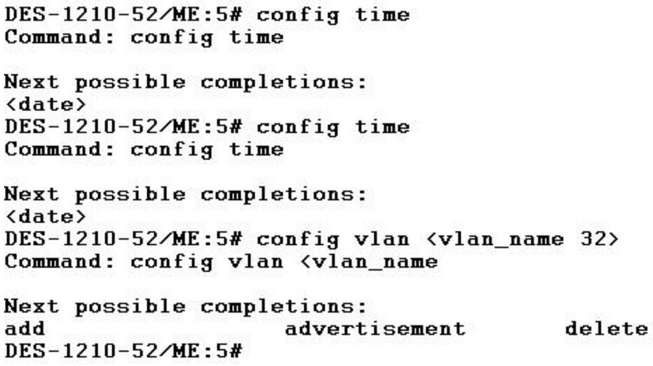
```
DES-1210-52/ME:5# config ipif
Command: config ipif

Next possible completions:
System
DES-1210-52/ME:5# config mirror
Command: config mirror

Next possible completions:
target
DES-1210-52/ME:5#
```

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 to enter the <username> with the message, command: config account. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

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

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



```
DES-1210-52/ME:5# config time
Command: config time

Next possible completions:
<date>
DES-1210-52/ME:5# config time
Command: config time

Next possible completions:
<date>
DES-1210-52/ME:5# config vlan <vlan_name 32>
Command: config vlan <vlan_name

Next possible completions:
add                   advertisement       delete
DES-1210-52/ME:5#
```

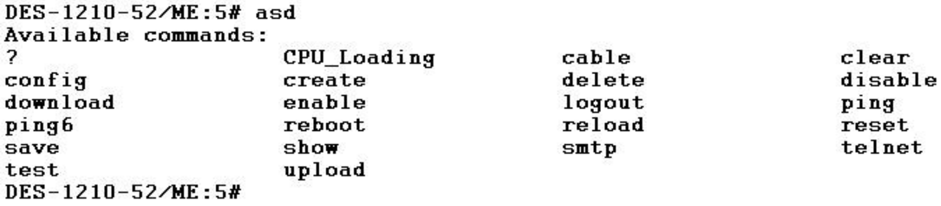
Figure 2–4 Using the Up Arrow to Re-enter a Command

In the above example, the command config account was entered without the required parameter <username>, the CLI returned the command: config account 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. The < > can also indicate a word with a number for character allowed.

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

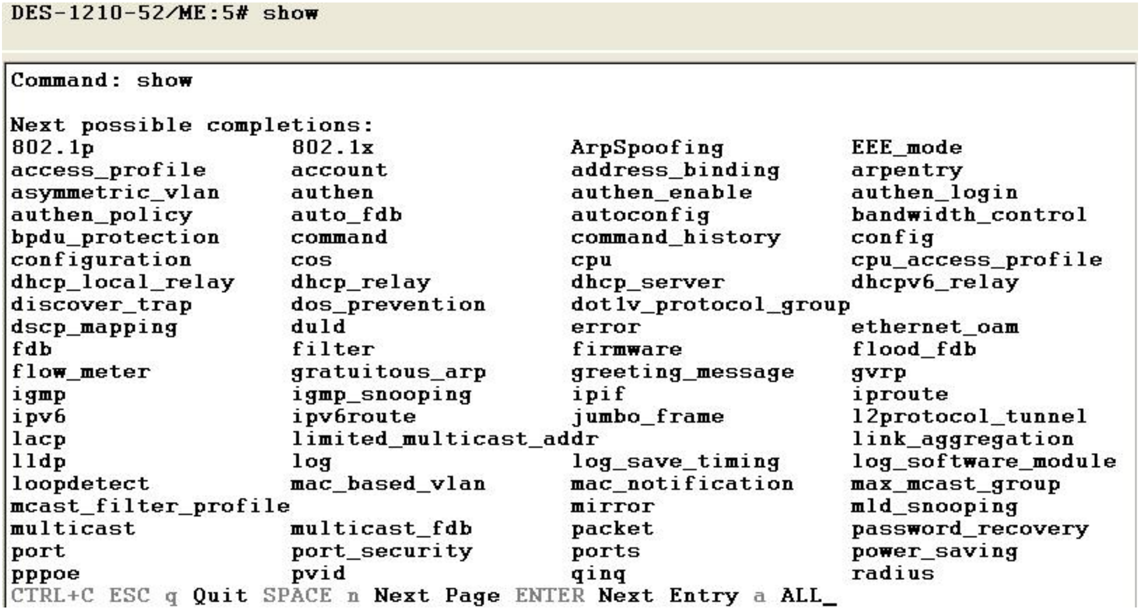


```
DES-1210-52/ME:5# asd
Available commands:
?                   CPU_Loading         cable               clear
config              create              delete              disable
download            enable              logout              ping
ping6               reboot              reload              reset
save                show                smtp                telnet
test                upload
DES-1210-52/ME:5#
```

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



```
DES-1210-52/ME:5# show

Command: show

Next possible completions:
802.1p              802.1x              ArpSpoofing         EEE_mode
access_profile      account             address_binding     arpentry
asymmetric_vlan     authen              authen_enable       authen_login
authen_policy       auto_fdb            autoconfig          bandwidth_control
bpdu_protection     command             command_history     config
configuration       cos                 cpu                 cpu_access_profile
dhcp_local_relay    dhcp_relay          dhcp_server         dhcpv6_relay
discover_trap       dos_prevention      dot1v_protocol_group
dscp_mapping        duld                error               ethernet_oam
fdb                 filter              firmware            flood_fdb
flow_meter          gratuitous_arp      greeting_message    gvrp
igmp                igmp_snooping       ipif                iproute
ipv6                ipv6route           jumbo_frame         l2protocol_tunnel
lacp                limited_multicast_addr                  link_aggregation
lldp                log                 log_save_timing     log_software_module
loopdetect          mac_based_vlan      mac_notification    max_mcast_group
mcast_filter_profile                    mirror              mld_snooping
multicast           multicast_fdb       packet              password_recovery
port                port_security       ports               power_saving
pppoe               pvid                qinq                radius
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL_
```

Figure 2–6 Next possible completions: Show Command

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

3

COMMAND SYNTAX

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

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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**create account [admin | operator | power-user |user] <username 15>**
Description	In the above syntax example, supply a username in the <username 15> space. Do not type the angle brackets.
Example Command	**create account admin newadmin1**

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	**create account [admin | operator | power-user |user] <username 15>**
Description	In the above syntax example, specify **admin, oper** or a **user** level account to be created. Do not type the square brackets.
Example Command	**create account user newuser1**

| vertical bar	
Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	**create account [admin | operator | power-user |user] <username 15>**
Description	In the above syntax example, specify **admin, oper,** or **user**. Do not type the vertical bar.
Example Command	**create account user newuser1**

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

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	reset
Description	execute “reset” will return the switch to its factory default setting.
Example command	reset Please be aware that all configuration will be reset to default value. Are you sure you want to proceed with system reset now? (Y/N)[N] N

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.
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 displays 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	Parameter
enable password encryption	
disable password encryption	
create account	[admin | operator | power-user | user] <username 15>
config account	<username 15>
show account	
delete account	<username 15>
show session	
show switch	
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	
enable clipaging	
disable clipaging	
enable web	{<tcp_port_number 1-65535>}
disable web	
enable autoconfig	
disable autoconfig	
save	{[config config_id <value 1-2> | log]}
reload config	config_id <value 1-2>
reboot	
reset	{[config | system | account | password | cpu]} {force_agree}
logout	
ping	<ipaddr> {times <value 1-255> | timeout <sec 1-99> | size <short 0-2080>}
ping6	<ipv6_addr> {frequency <sec 0-86400> | size <value 1-1522> | source_ip <ipv6_addr> | timeout <sec 1-99> | times <value 1-255>}
enable telnet	
disable telnet	
config time_range	<range_name 20> [[hours start_time <start_time 32> end_time <end_time 32>

Command	Parameter
	weekdays <daylist 32> date from_day year <start_year 2011-2029> month <start_mth 1-12> date <start_date 1-31> to_day year <end_year 2011-2029> month <end_mth 1-12> date <end_date 1-31>] | delete]
show time_range	
show tech support	
Clear tech support	

Each command is listed in detail, as follows:

enable password encryption

Purpose	Used to enable password encryption on a user account.
Syntax	**enable password encryption**
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system at a time in the future. If the password encryption is enabled, the password will be in encrypted form. If password encryption is disabled and the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enabled password encryption command, the password will still be in encrypted form. It can not revert back to plain text.
Parameters	None.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To enable password encryption on the Switch:

```
DES-1210-52/ME:5# enable password encryption
Command: enable password encryption


Success.

DES-1210-52/ME:5#
```

disable password encryption

Purpose	Used to disable password encryption on a user account.
Syntax	**disable password encryption**
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system at a time in the future. If the password encryption is enabled, the password will be in encrypted form. If password encryption is disabled and the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enabled password encryption command, the password will still be in encrypted form. It can not revert back to plain text.
Parameters	None.

Restrictions	Only Administrat level users can issue this command.

Example usage:

To disable password encryption on the Switch:

```
DES-1210-52/ME:5# disable password encryption
Command: disable password encryption



Success.

DES-1210-52/ME:5#
```

create account	
Purpose	To create user accounts.
Syntax	**create account [admin | operator | power-user | user] <username 15>**
Description	The **create account** command creates an administrator, operator, or user account that consists of a username and an optional password. Up to 31 accounts can be created. You can enter username and Enter. In this case, the system prompts for the account's password, which may be between 0 and 15 characters. Alternatively, you can enter the username and password on the same line.
Parameters	*admin* − Name of the administrator account. *opeator* − Specify an operator level account. *power-user* − Specify an power-user level account. *user* − Specify a user account with read-only permissions. *<username 1-15>* − The account username may be between 1 and 15 characters. *password* <password_string> {encrypted} - the account password can be included, and (optionally) can be encrypted.
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.

NOTE: You are not required to enter a User Name. However, if you do not enter a User Name, you cannot perform the following actions:

Create a monitor or operator (level 1 or level 14) users until an administrator user (level 15) is defined.

Delete the last administrator user if there are monitor and/or operator users defined.

Example usage:

To create an administrator-level user account with the username 'dlink':

```
DES-1210-52/ME:5# create account admin dlink
Command: create account admin dlink
```

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

Success.

DES-1210-52/ME:5#
```

config account

Purpose	To change the password for an existing user account.
Syntax	**config account <username 15>**
Description	The **config account** command changes the password for a user account that has been created using the **create account** command. The system prompts for the account’s new password, which may be between 0 and 15 characters.
Parameters	<*username 15*> − the account username.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user password of ‘dlink’ account:

```
DES-1210-52/ME:5# config account dlink
Enter a old password:****

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

Success.

DES-1210-52/ME:5#
```

show account

Purpose	To display information about all user accounts on the Switch.
Syntax	**show account**
Description	The **show account** command displays all account usernames and their access levels created on the Switch. Up to 31 user accounts can exist on the Switch at one time.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the account which have been created:

```
DES-1210-52/ME:5# show account
Command: show account


Username       Access Level
-----------------   --------------------
```

```
dlink              Admin

Total Entries : 1

DES-1210-52/ME:5#
```

delete account

Purpose	To delete an existing user account.
Syntax	**delete account <username 15>**
Description	The **delete account** command deletes a user account that has been created using the **create account** command.
Parameters	*<username 15>* − the account username.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account ‘System’:

```
DES-1210-52/ME:5# delete account System
Command: delete account System

Success.

DES-1210-52/ME:5#
```

reset account

Purpose	To deletes all the previously created accounts.
Syntax	**reset account**
Description	The **reset account** command deletes all the previously created accounts.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To deletes all the previously created accounts:

```
DES-1210-52/ME:5# reset account
Command: reset account


Are you sure to proceed with clean account?(y/n)y
Success.

DES-1210-52/ME:5#
```

show session	
Purpose	To display information about currently logged-in users.
Syntax	**show session**
Description	The **show session** command displays a list of all the users that are logged-in at the time the command is issued. The information includes the session ID (0 for the first logged-in user, 1 for the next logged-in user, etc.), the Protocol used to connect to the Switch, the user's IP address, the user's access Level (1=user, 15=admin), and the account name on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the way users logged in:

```
DES-1210-52/ME:5# show session
Command: show session

ID Live Time    From                                  Level   Name
--- ---------------  ------------------------------------- -------  ---------------
0  00:14:10     Serial Port                           5        anonymous

Total Entries: 1








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

show switch	
Purpose	To display information about the Switch.
Syntax	**show switch**
Description	The **show switch** command displays information about the Switch settings, including Device Type, MAC Address, IP configuration, Hardware/Software version, System information, and Switch Network configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch information:

```
DES-1210-52/ME:5# show switch
Command: show switch

Device Type                    : DES-1210-52/ME
MAC Address                     : 00-01-02-03-04-05
```

```
IP Address                      : 10.90.90.90 (Manual)
Subnet Mask                     : 255.0.0.0
Default Gateway                 : 0.0.0.0
System Boot Version             : 1.00.010
System Firmware Version         : 20.01.B082
System Hardware Version         : C1
System Serial Number            : QBDES12105200
System Name                     :
System Location                 :
System up time                  : 1 days, 23 hrs, 50 min, 34 secs
System Contact                  :
System Time                     : 02/01/2014 23:50:22
STP                             : Disabled
GVRP                            : Disabled
IGMP Snooping                   : Disabled
VLAN Trunk                      : Disabled
802.1X Status                   : Disabled
Telnet                          : Enabled (TCP 23)
Web                             : Enabled (TCP 80)
DES-1210-52/ME:5#
```

enable jumbo_frame

Purpose	To enable jumbo frames on the device.
Syntax	**enable jumbo_frame**
Description	The **enable jumbo_frame** command enables jumbo frames on the device.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command. Jumbo frames will be enabled after save and restart.

Example usage:

To enable jumbo frames:

```
DES-1210-52/ME:5# enable jumbo_frame
Command: enable jumbo_frame.

Success.
DES-1210-52/ME:5#
```

disable jumbo_frame

Purpose	To disable jumbo frames on the device.
Syntax	**disable jumbo_frame**
Description	The **disable jumbo_frame** command disables jumbo frames on the device.
Parameters	None.

Restrictions	Only Administrator or operate-level users can issue this command. Jumbo frames will be disabled after save and restart.

Example usage:

To disable jumbo_frames:

```
DES-1210-52/ME:5# disable jumbo_frame
Command: disable jumbo_frame

Success.
DES-1210-52/ME:5#
```

show jumbo_frame

Purpose	To display the jumbo frame configuration.
Syntax	**show jumbo_frame**
Description	The **show jumbo_frame** command displays the jumbo frame configuration.
Parameters	None.
Restrictions	None.

Example usage:

To show the jumbo_frames configuration status on the device:

```
DES-1210-52/ME:5# show jumbo_frame
Command: show jumbo_frame


Jumbo Frame is Enabled.
DES-1210-52/ME:5#
```

config bootrom password

Purpose	Used to configure the password when booting ROM.
Syntax	**config bootrom password <string20>**
Description	The **config bootrom password** command is used to configure the password when booting ROM.
Parameters	*<string 20>* - Specifies the password.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the boot ROM password:

```
DES-1210-52/ME:5# config bootrom password 1234
Command: config bootrom password 1234


Success.
DES-1210-52/ME:5#
```

enable clipaging

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

Example usage:

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

```
DES-1210-52/ME:5# enable clipaging
Command: enable clipaging

Success.
DES-1210-52/ME:5#
```

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when a command displays more than one screen of information.
Syntax	**disable clipaging**
Description	The **disable clipaging** command is used to disable the pausing of the console screen at the end of each page when a command would display more than one screen of information.
Parameters	None.
Restrictions	Only Administrator 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-1210-52/ME:5# disable clipaging
Command: disable clipaging

Success.
DES-1210-52/ME:5#
```

enable web

Purpose	To enable the HTTP-based management software on the Switch.
Syntax	**enable web {<tcp_port_number 1-65535>}**
Description	The **enable web** command enables the Web-based management software on the Switch. The user can specify the TCP port number the Switch uses 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 the TCP port number to listen for Telnet requests:

```
DES-1210-52/ME:5# enable web 80
Command: enable web 80

Success.

DES-1210-52/ME:5#
```

disable web

Purpose	To disable the HTTP-based management software on the Switch.
Syntax	**disable web**
Description	The **disable web** command disables 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-based management software on the Switch:

```
DES-1210-52/ME:5# disable web
Command: disable web

Success.

DES-1210-52/ME:5#
```

enable autoconfig

Purpose	Used to activate the auto configuration 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 auto configuration process the previously saved local configuration file present in Switch memory will be loaded. Only Administrator or operator-level users can issue this command.

Example usage:

To enable auto configuration on the Switch:

```
DES-1210-52/ME:5# enable autoconfig
Command: enable autoconfig



Success.
DES-1210-52/ME:5#
```

disable autoconfig

Purpose	Use this to deactivate auto configuration from DHCP.
Syntax	**disable autoconfig**
Description	The **disable autoconfig** command is used to instruct the Switch not to accept auto configuration 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 auto configuration function:

```
DES-1210-52/ME:5# disable autoconfig
Command: disable autoconfig



Success.
DES-1210-52/ME:5#
```

config autoconfig

Purpose	Use to configure the auto configuration timeout time from DHCP.
Syntax	**config autoconfig timeout <value 1-65535>**
Description	The **config autoconfig** command is used to the auto configuration timeout time from DHCP.
Parameters	*timeout <value 1-65535>* - Specifies the timeout time. And the value is from 1 to 65535 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the auto configuration timeout time to 100 seconds:

```
DES-1210-52/ME:5# config autoconfig timeout 100
Command: config autoconfig timeout 100
```

```

Success.
DES-1210-52/ME:5#
```

show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	**show autoconfig**
Description	The **show autoconfig** command is used to list the current status of the auto configuration function.
Parameters	None.
Restrictions	None.

Example usage:

To display the autoconfig status:

```
DES-1210-52/ME:5# show autoconfig
Command: show autoconfig

Autoconfig State: Disabled
Timeout           : 50 sec

DES-1210-52/ME:5#
```

enable auto learning

Purpose	To enable the MAC address auto learning on the switch.
Syntax	**enable auto learning**
Description	The **enable auto learing** command enables the MAC address auto learning feature on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable auto learning on the Switch:

```
DES-1210-52/ME:5# enable auto learning
Command: enable auto learning



Success.
DES-1210-52/ME:5#
```

disable auto learning

Purpose	To disable the MAC address auto learning of the switch.
Syntax	**disable auto learning**

Description	The **disable auto learing** command disables the MAC address auto learning feature on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable auto learning on the Switch:

```
DES-1210-52/ME:5# disable auto learning
Command: disable auto learning




Success.
DES-1210-52/ME:5#
```

save

Purpose	To save changes in the Switch’s configuration to non-volatile RAM.
Syntax	**save {[config config_id <value 1-2> | log]}**
Description	The **save** command 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* – Used to save the current configuration to a file. *config_id <value 1-2>* - Specifies which cfg file ID. if cfg ID is not specified, it refers to the boot_up CFG file. *log* – Used to save the current log to a file. The log file cannot be deleted.
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-1210-52/ME:5# save
Command: save

Building configuration ...
[OK]
DES-1210-52/ME:5#
```

reload config

Purpose	To reload the configuration of the Switch.
Syntax	**reload config config_id <value 1-2>**
Description	The **reload config** command allows user to reload the configuration of the Switch.
Parameters	*config_id <value 1-2>* - Specified the configuration id to be reloaded.
Restrictions	Only Administrator -level users can issue this command.

Example usage:

To reload the Switch:

```
DES-1210-52/ME:5# reload config config_id 1
Command: reload config config_id 1


Are you sure you want to reload the config?(y/n)y

% Reload config 1 Success.fully.

Are you sure you want to proceed with the system reboot?(y/n)y
% Please wait, the switch is rebooting...
```

reboot

Purpose	To reboot the Switch. If the Switch is a member of a stack, it may be rebooted individually, without affecting the other members of the stack.
Syntax	**reboot**
Description	The **reboot** command restarts the Switch.
Parameters	None.
Restrictions	Only Administrator -level users can issue this command.

Example usage:

To restart the Switch:

```
DES-1210-52/ME:5# reboot
Command: reboot



          DES-1210-52/ME Fast Ethernet Switch
                   Command Line Interface

                  Firmware: Build 20.01.B045
         Copyright(C) 2012 D-Link Corporation. All rights reserved.

DES-1210-52/ME UserName: System will Reboot....



U-Boot 2011.12.41872 (Feb 06 2015 - 19:32:31)

Board: RTL839x CPU:700MHz LXB:200MHz MEM:300MHz
DRAM:  256 MB
SPI-F: 1x32 MB
Loading 1024B env. variables from offset 0xc0000
Switch Model: RTL8353M_DEMO (Port Count: 52)
Switch Chip: RTL8353M
Model Info: 83536802
```

```
VLAN Init exclude CPU Port...
### RTL8208 config - MAC ID = 0 ###
### RTL8208 config - MAC ID = 8 ###
### RTL8208 config - MAC ID = 16 ###
### RTL8208 config - MAC ID = 24 ###
### RTL8208 config - MAC ID = 32 ###
### RTL8208 config - MAC ID = 40 ###
### RTL8214B Version C config - Phy0Id = 48 ###
[WARN] Serdes 1 initail fail bb00a478 10000
[WARN] Serdes 1 initail fail bb00a578 0
Please wait for PHY init-time ...

Net:   Net Initialization Skipped
rtl8390#0
Model_Name=DES-1210-52ME
==========================================
Hit any key to stop autoboot:  0
Verifying Checksum ...
BOOT:...OK
OS:...OK
FS:...OK
OS:...OK
FS:...OK
Boot/OS/FS Version:...OK
## Booting kernel from Legacy Image at b4100000 ...
   Image Name:
   Created:      2015-02-06  19:40:17 UTC
   Image Type:   MIPS Linux Kernel Image (gzip compressed)
   Data Size:    933753 Bytes = 911.9 KB
   Load Address: 80000000
   Entry Point:  80222000
   Verifying Checksum ... OK
*** Now go to linux runtime. ***
VLAN Init exclude CPU Port...
   Uncompressing Kernel Image ... OK

Starting kernel ...

Linux version 2.6.19 (george@206Server) (gcc version 3.4.4 mipssde-6.03.00-
20051020) #2 PREEMPT Fri Feb 6 19:40:09 CST 2015
CPU revision is: 00019555
Determined physical RAM map:
 memory: 02000000 @ 00000000 (usable)
User-defined physical RAM map:
 memory: 0f900000 @ 00000000 (usable)
Built 1 zonelists.  Total pages: 63246
Kernel command line: console=ttyS0,115200 mem=249M noinitrd
root=/dev/mtdblock3 rw rootfstype=squashfs csb=0x0116B56D cso=0x07979261
```

```
csf=0x388E21CF bid=DES-1210-52ME/C1 ethaddr=00:01:02:03:04:05
Primary instruction cache 32kB, physically tagged, 4-way, linesize 32 bytes.
Primary data cache 32kB, 4-way, linesize 32 bytes.
Synthesized TLB refill handler (20 instructions).
Synthesized TLB load handler fastpath (32 instructions).
Synthesized TLB store handler fastpath (32 instructions).
Synthesized TLB modify handler fastpath (31 instructions).
Cache parity protection disabled
PID hash table entries: 1024 (order: 10, 4096 bytes)
Dentry cache hash table entries: 32768 (order: 5, 131072 bytes)
Inode-cache hash table entries: 16384 (order: 4, 65536 bytes)
Memory: 250240k/254976k available (1788k kernel code, 4584k reserved, 391k data,
104k init, 0k highmem)
Mount-cache hash table entries: 512
Checking for 'wait' instruction...  available.
NET: Registered protocol family 16
NET: Registered protocol family 2
IP route cache hash table entries: 2048 (order: 1, 8192 bytes)
TCP established hash table entries: 8192 (order: 3, 32768 bytes)
TCP bind hash table entries: 4096 (order: 2, 16384 bytes)
TCP: Hash tables configured (established 8192 bind 4096)
TCP reno registered
squashfs: version 3.3 (2007/10/31) Phillip Lougher
JFFS2 version 2.2. (NAND) (C) 2001-2006 Red Hat, Inc.
io scheduler noop registered
io scheduler anticipatory registered
io scheduler deadline registered
io scheduler cfq registered (default)
Serial: 8250/16550 driver $Revision: 1.90 $ 1 ports, IRQ sharing disabled
serial8250: ttyS0 at MMIO 0x0 (irq = 31) is a 16550A
Creating 8 MTD partitions on "Total SPI FLASH":
0x00000000-0x000c0000 : "BOOT"
0x000c0000-0x00100000 : "BDINFO"
0x00100000-0x00280000 : "KERNEL1"
0x00280000-0x00e80000 : "ROOTFS1"
0x00e80000-0x01000000 : "KERNEL2"
0x01000000-0x01040000 : "SYSINFO"
0x01040000-0x01c40000 : "ROOTFS2"
0x01c40000-0x02000000 : "JFFS2"
memmap_pid load
TCP cubic registered
NET: Registered protocol family 1
NET: Registered protocol family 17
VFS: Mounted root (squashfs filesystem) readonly.
Freeing unused kernel memory: 104k freed
init started:  BusyBox v1.00 (2015.02.06-11:36+0000) multi-call binary
Starting pid 14, console : '/etc/rc'
Init RTCORE Driver Module....OK                         100%
```

```
  MAC Address : 00-01-02-03-04-05
  H/W Version :
  F/W Version : 20.01.B045

 Complete NpHwInit
RTK.0>
.........................................................



                    DES-1210-52/ME Fast Ethernet Switch
                        Command Line Interface

                       Firmware: Build 20.01.B045
             Copyright(C) 2012 D-Link Corporation. All rights reserved.

DES-1210-52/ME UserName:
```

reset	
Purpose	To reset the Switch to the factory default settings.
Syntax	**reset {[config | system | account | password | cpu]} {force_agree}**
Description	The **reset** command restores the Switch’s configuration to the default settings assigned from the factory. Execution of the **reset** command through the CLI retains the unit’s current stack membership number.
Parameters	*config* - If the keyword ‘config’ is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, and the switch history log. The Switch will not save or reboot. *system* − If the keyword ‘system’ is specified all of the factory default settings are restored on the Switch. The Switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base. *account* − If the keyword ‘account is specified, all of the factory default account settings are restored on the Switch. *password* − If the keyword ‘password is specified, all of the factory default password settings are restored on the Switch. *cpu* - If the keyword ‘cpu is specified, all of the factory default cpu settings are restored on the Switch. *{force_agree}* - When force_agree is specified, the reset command will be executed immediately without further confirmation. If no parameter is specified, the Switch’s current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The Switch will not save or reboot.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To restore all of the Switch’s configuration to their default values:

```
DES-1210-52/ME:5# reset config force_agree
Command: reset config force_agree



Success.
DES-1210-52/ME:5#
```

logout

Purpose	To log out a user from the Switch's console.
Syntax	**Logout**
Description	The **logout** 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-1210-52/ME:5#  logout
```

ping

Purpose	To test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value 1-255> | timeout <sec 1-99> | size <short 0-2080>}**
Description	The **ping** command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address then 'echos' or returns the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters	*<ipaddr>* - The IP address of the host. *times <value 1-255>* - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4. *timeout <sec 1-99>* - 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. *size <short 0-2080>* - Specify the size of the test packet. A value of 0 to 2080 can be specified.
Restrictions	None.

Example usage:

To ping the IP address 10.90.90.97 ten times with timeout 3 seconds:

```
DES-1210-52/ME:5# ping 10.90.90.97 times 10 timeout 3
Command: ping 10.90.90.97 times 10 timeout 3

Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs

--- 10.90.90.97 Ping Statistics ---
10 Packets Transmitted, 0 Packets Received, 100% Packets Loss
DES-1210-52/ME:5#
```

ping6

Purpose	To test the IPv6 connectivity between network devices.
Syntax	**ping6 <ipv6_addr> {frequency <sec 0-86400> | size <value 1-1522> | source_ip <ipv6_addr> | timeout <sec 1-99> | times <value 1-255>}**
Description	The **ping6** command sends IPv6 Internet Control Message Protocol (ICMP) echo messages to a remote IPv6 address. The remote IPv6 address will then "echo" or return the message. This is used to confirm the IPv6 connectivity between the switch and the remote device.
Parameters	*<ipv6_addr>* - The IPv6 address of the host. *frequency <sec 0-86400>* - The number of seconds to wait before repeating a ping test as defined by the value of this parameter. A single ping test consists of a series of ping probes. The number of probes is determined by the value of the parameter times. After a single test completes the number of seconds as defined by the value of frequency must elapse before the next ping test is started. A value of 0 for this parameter implies that the test as defined by the corresponding entry will not be repeated. *size <short 1-1522>* - Specify the size of the test packet. A value of 1 to 6000 can be specified. *source_ip <ipv6_addr >* - Specify the source IPv6 address of the ping packets. If specified this parameter, this IPv6 address will be used as the packets' source IPv6 address that ping6 sends to the remote host. *timeout <sec 1-99>* - 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. *times <value 1-255>* - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4.
Restrictions	None.

Example usage:

To ping the IPv6 address to "3000::1" four times:

```
DES-1210-52/ME:5# ping6 3000::1 times 4
Command: ping6 3000::1 times 4

Reply From : 3000::1, bytes=200, time<10ms
Reply From : 3000::1, bytes=200, time<10ms
Reply From : 3000::1, bytes=200, time<10ms
Reply From : 3000::1, bytes=200, time<10ms


--- 3000::1 Ping Statistics ---
4 Packets Transmitted, 4 Packets Received, 0% Packets Loss
DES-1210-52/ME:5#
```

traceroute

Purpose	The traceroute User EXEC mode command discovers routes that packets actually take when traveling to their destination.
Syntax	**traceroute <ip_addr> {[max-ttl <short 1-99> | min-ttl <short 1-99>}**
Description	The **traceroute** command discovers routes that packets actually take when traveling to their destination.
Parameters	*<ip_addr>* - Specifies the IP address of the destination host. *max-ttl <short 1-99> - The largest TTL value that can be used. The traceroute command terminates when the* destination is reached or when this value is reached. *min-ttl <short 1-99> - The smallest TTL value that can be used. The traceroute command terminates when the* destination is reached or when this value is reached.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To trace route IP 10.90.90.92 with max-ttl is 10:

```
DES-1210-52/ME:5# traceroute 10.90.90.92 max-ttl 10
Command: traceroute 10.90.90.92 max-ttl 10

Tracing Route to 10.90.90.92 with 10 hops max and 1 byte packets
[!N - Network Unreachable !H - Host Unreachable !P - Protocol Unreachable]
  1    0.0.0.0              *              *        *
  2    0.0.0.0              *              *        *
  3    0.0.0.0              *              *        *
  4    0.0.0.0              *              *        *
  5    0.0.0.0              *              *        *
  6    0.0.0.0              *              *        *
  7    0.0.0.0              *              *        *
  8    0.0.0.0              *              *        *
  9    0.0.0.0              *              *        *
 10    0.0.0.0               *              *        *
DES-1210-52/ME:5#
```

traceroute6

Purpose	The traceroute User EXEC mode command discovers routes that packets actually take when traveling to their destination.

Syntax	**traceroute6 <ipv6_addr> {[max-ttl <short 1-99> | min-ttl <short 1-99>}**
Description	The **traceroute6** command discovers routes that packets actually take when traveling to their destination.
Parameters	*<ipv6_addr>* - Specifies the IPv6 address of the destination host. *max-ttl <short 1-99> - The largest TTL value that can be used. The traceroute command terminates when the* destination is reached or when this value is reached. *min-ttl <short 1-99> - The smallest TTL value that can be used. The traceroute command terminates when the* destination is reached or when this value is reached.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To trace route IPv6 3000::2 with max-ttl is 8:

```
DES-1210-52/ME:5# traceroute6 3000::2 max-ttl 8
Command: traceroute6 3000::2 max-ttl 8

Tracing Route to 3000::2 with 8 hops max and 1 byte packets
[!N - Network Unreachable !H - Host Unreachable !P - Protocol Unreachable]
 1     ::                     *       *       *
 2     ::                     *       *       *
 3     ::                     *       *       *
 4     ::                     *       *       *
 5     ::                     *       *       *
 6     ::                     *       *       *
 7     ::                     *       *       *
 8     ::                     *       *       *
DES-1210-52/ME:5#
```

show cpu port

Purpose	To display the CPU port information.
Syntax	**show cpu port**
Description	The **show cpu port** command displays the CPU port information.
Parameters	None.
Restrictions	Only Administrator users can issue this command.

Example usage:

To display the CPU port information:

```
DES-1210-52/ME:5# show cpu port
Command: show cpu port

Type                  Total     Diff
--------------------------  ---------- -----------
ARP                    0
DHCP                   0
DHCPv6                 0
```

```
GVRP                0
ICMP                0
ICMPv6              0
IGMP                0
LACP                0
LLDP                0
PPPoE               0
Reserved Multicast  0
STP                 0
TELNET              0
UDP                 0


DES-1210-52/ME:5#
```

reset cpu port

Purpose	To reset the CPU port information.
Syntax	**reset cpu port**
Description	The **reset cpu port** command resets the CPU port information.
Parameters	None.
Restrictions	Only Administrator users can issue this command.

Example usage:

To reset the CPU port information:

```
DES-1210-52/ME:5# reset cpu port
Command: reset cpu port

Success.

DES-1210-52/ME:5#
```

enable telnet

Purpose	To enable the telnet.
Syntax	**enable telnet**
Description	The **enable telnet** command enables telnet.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To enable telnet:

```
DES-1210-52/ME:5# enable telnet
Command: enable telnet


Success.
```

```
DES-1210-52/ME:5#
```

disable telnet

Purpose	To disable telnet.
Syntax	**disable telnet**
Description	The **disable telnet** command disables telnet.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To disable telnet:

```
DES-1210-52/ME:5# disable telnet
Command: disable telnet

Success.

DES-1210-52/ME:5#
```

telnet

Purpose	To telnet another device.
Syntax	**telnet <ipaddr> {-l <string>}**
Description	The **telnet** command is used to telnet another device.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To telnet another device which IP is 10.90.90.91:

```
DES-1210-52/ME:5# telnet 10.90.90.91
Command: telnet 10.90.90.91
```

config time_range

Purpose	To configure the time range on the Switch.
Syntax	**config time_range <range_name 20> [[hours start_time <start_time 32> end_time <end_time 32> weekdays <daylist 32> date from_day year <start_year 2011-2029> month <start_mth 1-12> date <start_date 1-31> to_day year <end_year 2011-2029> month <end_mth 1-12> date <end_date 1-31>] | delete]**
Description	The **config time_range** command defines time ranges for access lists. If the end time is earlier than the start time, the end time will move to the following day
Parameters	*<range_name 20>* – Specifies the time range name. The range of characters is 1 - 20. *start_time <start_time 32>* – defines the time on which the time range will start to be active.

	end_time <end_time 32 >– defines the time on which the time range will stop to be active. *weekdays <daylist 32>* – defines the days of the week on which the time range will be active. <*start_year 2011-2029* > – Specifies the time range start year. <*start_mth 1-12*> – Specifies the time range start month. <*start_date 1-31*> – Specifies the time range start date. <*end_year 2011-2029* > – Specifies the time range end year. <*end _mth 1-12*> – Specifies the time range end month. <*end _date 1-31*> – Specifies the time range end date. *delete* – Delete the time range settings.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the time range on the Switch:

```
DES-1210-52/ME:5# config time_range dd hours start_time 00:22 end_time
12:34 weekdays tue-fri date from_day year 2012 month 1 date 1 to_day year
2012 month 1 date 3
Command: config time_range dd hours start_time 00:22 end_time 12:34
weekdays tue-fri date from_day year 2012 month 1 date 1 to_day year 2012
month 1 date 3



Success!
DES-1210-52/ME:5#
```

show time_range

Purpose	To display the currently configured access profiles on the Switch.
Syntax	**show time_range**
Description	The **show time_range** command displays the time range configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display time range settings on the Switch:

```
DES-1210-52/ME:5# show time_range

Range name   : xxx
Start time   : 10:00
End time      : 11:00
Days         : wed sun

Total Entries : 1

DES-1210-52/ME:5#
```

show tech support

Purpose	To display system and configuration information. to provide to the Technical Assistance Center when reporting a problem, use the show tech-support command.
Syntax	**show tech support**
Description	The **show tech support** command displays system and configuration information. to provide to the Technical Assistance Center when reporting a problem. By default, this command displays the output for technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data. The **show tech support** command may time out if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a set logout *timeout* value of 0 to disable automatic disconnection of idle sessions or enter a longer *timeout* value. The **show tech support** command output is continuous; it does not display one screen at a time. To interrupt the output, press Esc.
Parameters	None.
Restrictions	None.

Example usage:

To display technical support information on the Switch:

```
DES-1210-52/ME:5# show tech support
Command: show tech support



- Stacktrace Log -

No stacktrace information.

- System Info. -

Device Type                     : DES-1210-52/ME
MAC Address                      : 00-01-02-03-04-05
IP Address                      : 10.90.90.90 (Manual)
Subnet Mask                     : 255.0.0.0
Default Gateway                 : 0.0.0.0
System Boot Version             : 1.00.010
System Firmware Version         : 20.01.B045
System Hardware Version          : C1
System Serial Number            : QBDES12105200
System Name                      :
System Location                 :
System up time                  : 0 days, 0 hrs, 34 min, 56 secs
System Contact                  :
System Time                     : 01/01/2014 00:34:44
```

```
STP                              : Disabled
GVRP                             : Disabled
IGMP Snooping                    : Disabled
VLAN Trunk                       : Disabled
802.1X Status                    : Disabled
Telnet                           : Enabled (TCP 23)
Web                              : Enabled (TCP 80)
RMON                             : Disabled
SSH                              : Disabled
Syslog Global State              : Disabled
SSL                              : Disabled
CLI Paging                       : Enabled
Password Encryption State        : Disabled


- Memory Info. -

          total     used     free    shared   buffers
Mem:      250496    99844    150652      0      5232
Swap:          0        0         0
Total:    250496    99844    150652
DES-1210-52/ME:5#
```

clear tech support	
Purpose	To clear system and configuration information.
Syntax	**clear tech support**
Description	The **clear tech support** command is used to clear system and configuration information.
Parameters	None.
Restrictions	None.

Example usage:

To clear technical support information on the Switch:

```
DES-1210-52/ME:5# clear tech support
Command: clear tech support


Success.
DES-1210-52/ME:5#
```

5

DHCP AUTOIMAGE COMMANDS

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

Command	Parameter
enable autoimage	
diable autoimage	
show autoimage	

Each command is listed in detail, as follows:

enable autoimage

Purpose	To enable the DHCP automatic image function on the Switch.
Syntax	**enable autoimage**
Description	The **enable autoimage** command is used to enable the DHCP automatic image function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the DHCP automatic image function on the Switch:

```
DES-1210-52/ME:5# enable autoimage
Command: enable autoimage


Success.
DES-1210-52/ME:5#
```

disable autoimage

Purpose	To disable the DHCP automatic image function on the Switch.
Syntax	**disable autoimage**
Description	The **disable autoimage** command is used to disable the DHCP automatic image function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the DHCP automatic image function on the Switch:

```
DES-1210-52/ME:5# disable autoimage
Command: disable autoimage



Success.
DES-1210-52/ME:5#
```

show autoimage

Purpose	To display the DHCP automatic image function on the Switch.
Syntax	**show autoimage**
Description	The **disable autoimage** command is used to display the DHCP automatic image function on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP automatic image information on the Switch:

```
DES-1210-52/ME:5# show autoimage
Command: show autoimage

Autoimage State: Enabled
DES-1210-52/ME:5#
```

6

SMTP SERVER COMMANDS

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

Command	Parameter
enable smtp	
disable smtp	
config smtp	[self_mail_addr <mail_addr 64> | server [<ipaddr> | <ipv6addr>] | server_port <tcp_port_number 1-65535>] [{add mail_receiver <mail_addr 64>| delete mail_receiver <index 1-8>}]
show smtp	
smtp sent_testmsg	

Each command is listed in detail, as follows:

enable smtp	
Purpose	To enable the SMTP server feature on the Switch.
Syntax	**enable smtp**
Description	The **enable smtp** command enables the SMTP server feature on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable SMTP feature on the Switch:

```
DES-1210-52/ME:5# enable smtp
Command: enable smtp

Success.
DES-1210-52/ME:5#
```

disable smtp	
Purpose	To disable the SMTP server feature on the Switch.
Syntax	**disable smtp**
Description	The **disable smtp** command disables the SMTP server feature on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable STMP feature on the Switch:

```
DES-1210-52/ME:5# disable smtp
Command: disable smtp

Success.
DES-1210-52/ME:5#
```

config smtp

Purpose	To configure the fields to set up the SMTP server for the switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.
Syntax	**config smtp [self_mail_addr <mail_addr 64> | server [<ipaddr> | <ipv6addr>] | server_port <tcp_port_number 1-65535>] [{add mail_receiver <mail_addr 64>| delete mail_receiver <index 1-8>}]**
Description	The **config smtp** command is used to configure the fields to set up the SMTP server for the switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.
Parameters	*self_mail_addr <mail_addr 64>* − Specifies the e-mail address from which mail messages will be sent. Only one self mail address can be configured on the Swtich. *server [<ipaddr>* | *<ipv6addr>]* − Specifies the IPv4 or IPv6 address of the SMTP server. This will be the device that sends out the mail for user. For example, 10.90.90.99. *<tcp_port_number 1-65535>* − Specifies the port number that the Switch will connect with on the SMTP server. The range is between 1 and 65535. *add mail_receiver <mail_addr 64>* − Specifies a list of e-mail addresses so recipients can receive e-mail messages regarding Switch functions. Up to 8 e-mail address can be added per Switch. *delete mail_receiver <index 1-8>* − Specifies the e-mail address index to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config SMTP with self mail address ‘dlink@mail.com.tw’ on the Switch:

```
DES-1210-52/ME:5# config smtp self_mail_addr dlink@mail.com.tw
Command: config smtp self_mail_addr dlink@mail.com.tw


Success.
DES-1210-52/ME:5#
```

show smtp

Purpose	To display the SMTP server settings on the Switch.

Syntax	**show smtp**
Description	The **show smtp** command displays the SMTP server settings on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display SMTP information on the Switch:

```
DES-1210-52/ME:5# show smtp
Command: show smtp

smtp status : Enable
smtp server address : 0.0.0.0
smtp server port : 25
self mail address : dlink@mail.com.tw

Index          Mail Receiver Address
--------      -------------------------------------
1
2
3
4
5
6
7
8

DES-1210-52/ME:5#
```

smtp sent_testmsg

Purpose	To send test messages to all mail recipients configured on the Switch.
Syntax	**smtp sent_testmsg**
Description	The **smtp sent_testmsg** command is used to send test messages to all mail recipients configured on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To send SMTP test message to all mail receivers:

```
DES-1210-52/ME:5# smtp sent_testmsg
Command: smtp sent_testmsg

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

```

Sending mail, please wait...

Success.

DES-1210-52/ME:5#
```

7

MODIFY BANNER AND PROMPT COMMANDS

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

Command	Parameter
config command_prompt	[<string 32> | default | username]
config greeting_message	{default}
show greeting_message	

Each command is listed in detail, as follows:

config command_prompt	
Purpose	To configure the command prompt.
Syntax	**config command_prompt [<string 32> | default | username]**
Description	The **config command_prompt** command configures the command prompt.
Parameters	*<string 32>* – The command prompt can be changed by entering a new name of no more that 32 characters. *default* – The command prompt will reset to factory default command prompt. Default = the name of the Switch model, for example “DES-1210-52”. *username* – The command prompt will be changed to the login username.
Restrictions	Only Administrator and Operator-level users can issue this command. Other restrictions include: If the “reset” command is executed, the modified command prompt will remain modified. However, the “reset config/reset system” command will reset the command prompt to the original factory banner.

Example usage:

To modify the command prompt to “AtYourService”:

```
DES-1210-52/ME:5# config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:5#
```

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

Example usage:

```
Command: config greeting_message

Greeting Messages Editor
================================================================================

                 DES-1210-52/ME Fast Ethernet Switch
                    Command Line Interface

                   Firmware: Build 20.01.B045
         Copyright(C) 2012 D-Link Corporation. All rights reserved.

================================================================================

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

show greeting_message

Purpose	Used to view the currently configured greeting message configured on the Switch.
Syntax	**show greeting_message**
Description	The **show greeting_message** 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-1210-52/ME:5# show greeting_message
Command: show greeting_message

             DES-1210-52/ME Fast Ethernet Switch
                    Command Line Interface

                   Firmware: Build 20.01.B045
          Copyright(C) 2012 D-Link Corporation. All rights reserved.

DES-1210-52/ME:5#
```

8

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	Parameter
config ports	[all | <portlist>] medium_type [copper | fiber] MDI/MDIX [MDI | MDIX | auto] {clear_description | description <desc 32> | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | speed [auto | 1000_full | 100_full | 100_half | 10_full | 10_half]}
config ports	[all | <portlist>] capability_advertised [1000_full | 100_full | 100_half | 10_full | 10_half | 10G_full] {[1000_full | 100_full | 100_half | 10_full | 10_half]}
show ports	{<portlist> | all} {description | err_disabled | linkup_time | auto_negotiation | media_type}
delete ports	[<portlist> | all] {medium_type [copper | fiber]} description

Each command is listed in detail, as follows:

config ports	
Purpose	To configure the Switch’s Ethernet port settings.
Syntax	**config ports [all | <portlist>] medium_type [copper | fiber] MDI/MDIX [MDI | MDIX | auto] {clear_description | description <desc 32> | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | speed [auto | 1000_full | 100_full | 100_half | 10_full | 10_half]}**
Description	The **config ports** command configures the Switch’s Ethernet port settings. Only the ports listed in the <portlist> are affected.
Parameters	*<portlist>* − A port or range of ports to be configured. *all* − Configures all ports on the Switch. *medium_type [copper | fiber]* − If configuring the Combo ports, this defines the type of medium being configured. *MDI/MDIX [MDI | MDIX | j auto]* − Specifies the MDI or MDIX setting of the port. The MDIX setting can be auto, normal or cross. If set to normal state, the port in MDIX mode, can be connected to PC NIC using a straight cable. If set to cross state, the port in mdi mode, can be connected to a port (in mdix mode) on another switch through a straight cable. *clear_description* − Clear the description of selected port. *description <desc 32>* − Enter and alphanumeric string of no more that 32 characters to describe a selected port interface. *flow_control [enable]* – Enables flow control for the specified ports. *flow_control [disable]* – Disables flow control for the specified ports. *learning [enable | disable]* c Enables or disables the MAC address learning on the specified range of ports. *state [enable | disable]* − Enables or disables the specified range of

	ports. *speed* – Sets the speed of a port or range of ports, with the addition of one of the following: • *auto* − Enables auto-negotiation for the specified range of ports. • *[10 | 100 | 1000]* − Configures the speed in Mbps for the specified range of ports. • *[half* | *full]* − Configures the specified range of ports as either full or half-duplex.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the speed of ports 1-3 to be 100 Mbps, full duplex, learning and state enabled:

```
DES-1210-52/ME:5# config ports 1-3 medium_type copper speed 100_full learning
enable state enable
Command: config ports 1-3 medium_type copper speed 100_full learning enable
state enable

Success.

DES-1210-52/ME:5#
```

config ports	
Purpose	To configure the Switch's Ethernet port settings.
Syntax	**config ports [all | <portlist>] capability_advertised [1000_full | 100_full | 100_half | 10_full | 10_half | 10G_full] {[1000_full | 100_full | 100_half | 10_full | 10_half]}**
Description	The **config ports** command configures the Switch's Ethernet port settings. Only the ports listed in the <portlist> are affected.
Parameters	*<portlist>* − A port or range of ports to be configured. *all* − Configures all ports on the Switch. *speed* – Sets the speed of a port or range of ports, with the addition of one of the following: • *[10 | 100 | 1000 | 10G]* − Configures the speed in Mbps for the specified range of ports. • *[half* | *full]* − Configures the specified range of ports as either full or half-duplex.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the speed of ports 8-11 to be 10G full Mbps:

```
DES-1210-52/ME:5# config ports 8-11 capability_advertised 10G_full
Command: config ports 8-11 capability_advertised 10G_full



Success
```

```
DES-1210-52/ME:5#
```

show ports

Purpose	To display the current configuration of a range of ports.
Syntax	**show ports {<portlist> | all} {description | err_disabled | linkup_time | auto_negotiation | media_type}**
Description	The **show ports** command displays the current configuration of a port or range of ports.
Parameters	*<portlist>* − A port or range of ports whose settings are to be displayed. *all* – Specifies all ports to be displayed. *linkup_time* – Specifies to display the linkup time information of specified ports. *auto_negotiation* – Specifies to display the port auto-negotiation information. *media_type* – Specifies to display the media type of the port.
Restrictions	None.

Example usage:

To display the configuration of port 8 on the Switch:

```
DES-1210-52/ME:5# show ports 8
Command: show ports 8

Port  State/    Settings                 Connection               Address
Type  MDI       Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    Learning
-----  -------  -----------------------  -----------------------  ------------
8     Enabled   Auto/Disabled             Link Down               Enabled
      Auto

DES-1210-52/ME:5#
```

delete ports

Purpose	To delete the current information of ports.
Syntax	**delete ports [<portlist> | all] {medium_type [copper | fiber]} description**
Description	The **delete ports** command deletes the current information of a port or range of ports.
Parameters	*[<portlist>* | *all]* – Specifies a range of ports or all ports information to be deleted. *medium_type [copper* | *fiber]* – Specifies to delete the medium type of specified ports. *description* – Specifies to delete the description of specified ports.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete the description of ports 1-3:

```
DES-1210-52/ME:5# delete ports 1-3 description
Command: delete ports 1-3 description

DES-1210-52/ME:5#
```

9

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	Parameter
enable loopdetect	
disable loopdetect	
config loopdetect mode	[portbase | vlanbase]
config loopdetect ports	[<portlist> | all] state [enable | disable]
config loopdetect	interval_time <value 1-32767> lbd_recover_time [0 | <value 60-1000000>]
show loopdetect	{ports [<portlist> | all]}

Each command is listed in detail, as follows:

enable loopdetect	
Purpose	To enable the loop back detection on the Switch.
Syntax	**enable loopdetect**
Description	The **enable loopdetect** command enables the loop back detection on the Switch.
Parameters	None.
Restrictions	Only administrator -level users can issue this command.

Example usage:

To enable the loopback detection feature on the Switch:

```
DES-1210-52/ME:5# enable loopdetect
Command: enable loopdetect



Success.
DES-1210-52/ME:5#
```

disable loopdetect	
Purpose	To disable the loop back detection on the Switch.
Syntax	**disable loopdetect**
Description	The **disable loopdetect** command disables the loop back detection on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the loopback detection feature on the Switch:

```
DES-1210-52/ME:5# disable loopdetect
Command: disable loopdetect



Success.
DES-1210-52/ME:5#
```

config loopdetect mode

Purpose	To configure the loop back detection mode to be portbase or vlanbase on the Switch.
Syntax	**config loopdetect mode [portbase | vlanbase]**
Description	The **config loopdetect mode** command configures loop back detection mode to be portbase or vlanbase on the Switch.
Parameters	*[portbase | vlanbase]]* - Specifies the loopdetect mode to be portbase or vlanbase.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the loopback detection mode to be portabse on the Switch:

```
DES-1210-52/ME:5# config loopdetect mode portbase
Command: config loopdetect mode portbase



Success.
DES-1210-52/ME:5#
```

config loopdetect ports

Purpose	To configures the loop back detection to be enabled or disabled for the specific ports on the Switch.
Syntax	**config loopdetect ports [<portlist> | all] state [enable | disable]**
Description	The **config loopdetect ports** command configures the loop back detection to be enabled or disabled for the specific ports on the Switch.
Parameters	*<portlist>* − A port or range of ports to be configured. *all* − All ports settings are to be configured. *state [enabled | disabled]* − Specifies the loop back detection is enabled or disabled for the specified ports on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable the loop back detection on the Switch:

```
DES-1210-52/ME:5# config loopdetect ports all enable
Command: config loopdetect ports all enable

```

```

Success.
DES-1210-52/ME:5#
```

config loopdetect

Purpose	To configure the loop back detection interval time and recover time on the Switch.
Syntax	**config loopdetect interval_time <value 1-32767> lbd_recover_time [0 | <value 60-1000000>]**
Description	The **config loopdetect** command configures the loop back detection interval time and recover time on the Switch.
Parameters	*interval_time <value 1-32767>* − Specifies the interval time of loop back detection. The range is between 1 and 32767 seconds. *lbd_recover_time [0 | <value 60-10000>]* − Specifies the recover time of loop back detection on the switch. The range is between 60 and 10000 seconds.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the loop back detection with interval time 500 on the Switch:

```
DES-1210-52/ME:5# config loopdetect interval_time 500
Command: config loopdetect interval_time 500

Success.
DES-1210-52/ME:5#
```

show loopdetect

Purpose	To display the loop back detection information on the Switch.
Syntax	**show loopdetect {ports [<portlist> | all]}**
Description	The **show loopdetect** command displays the loop back detection information on the Switch.
Parameters	*<portlist>* − A port or range of ports to be displayed. *all* − All ports settings are to be displayed.
Restrictions	None.

Example usage:

To display the loop back detection information on the Switch:

```
DES-1210-52/ME:5# show loopdetect
Command: show loopdetect


 Loopdetect Global Settings


 ---------------------------------------
Loopdetect Status    : Enabled
Loopdetect Mode      : Port-Base
Loopdetect Interval   : 100
Recover Time           : 60
DES-1210-52/ME:5#
```

10

DOS PREVENTION COMMANDS

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

Command	Parameter
config dos_prevention dos_type	[{land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024} | all] {action [drop | mirror <port> {priority <value (0-7)> | rx_rate [no_limit | <value (64-1024000)>] }] | state [enable | disable]] }
show dos_prevention	{ land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }
enable dos_prevention trap_log	
disable dos_prevention trap_log	

Each command is listed in detail, as follows:

config dos_prevention dos_type

Purpose	Used to discard the L3 control packets sent to CPU from specific ports.
Syntax	**config dos_prevention dos_type [{land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024} | all] {action [drop | mirror <port> {priority <value (0-7)> | rx_rate [no_limit | <value (64-1024000)>] }] | state [enable | disable]] }**
Description	The **config dos_prevention dos_type** command is used to configure the prevention of DoS attacks, and includes state and action. The packets matching will be used by the hardware. For a specific type of attack, the content of the packet, regardless of the receipt port or destination port, will be matched against a specific pattern.
Parameters	The type of DoS attack. Possible values are as follows: land_attack, blat_attack, smurf_attack, tcp_null_scan, tcp_xmascan tcp_synfin and tcp_syn_srcport_less_1024. By default, prevention for all types of DoS are enabled except for tcp_syn_srcport_less_1024. *action [drop* | *mirror]* - When enabling DoS prevention, the following actions can be taken. *drop* – Drop the attack packets. *mirror* – Mirror the packet to other port for further process. *priority <value (0-7)>* – Change packet priority by the Switch from 0 to 7. If the priority is not specified, the original priority will be used.

	rx_rate [no_limit | *<value (64-1024000)>]* – controls the rate of the received DoS attack packets. If not specified, the default action is drop. *state [enable* | *disable]*- Enable or disable DoS prevention.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a land attack and blat attack prevention:

```
DES-1210-52/ME:5# config dos_prevention dos_type blat_attack action
drop
Command: config dos_prevention dos_type blat_attack action drop



Success.

DES-1210-52/ME:5#
```

show dos_prevention

Purpose	Used to display DoS prevention information.
Syntax	**show dos_prevention { land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }**
Description	The **show dos_prevention** command is used to display DoS prevention information, including the type of DoS attack, the prevention state, the corresponding action if the prevention is enabled, and the counter information of the DoS packet.
Parameters	The type of DoS attack. Possible values are as follows: land_attack, blat_attack, smurf_attack, tcp_null_scan, tcp_xmascan tcp_synfin and tcp_syn_srcport_less_1024.
Restrictions	None.

Example usage:

To display DoS prevention information:

```
DES-1210-52/ME:5# show dos_prevention
Command: show dos_prevention

Trap/Log   : Disabled
DosType                      State     Action         Frame Counts
-------------------------    --------  ------------   -------------------
Land Attack                  Disabled  Drop             -
Blat Attack                  Disabled  Drop             -
Smurf Attack                 Disabled  Drop             -
Tcp Null Scan                Disabled  Drop             -
Tcp Xmascan                  Disabled  Drop             -
Tcp Synfin                   Disabled  Drop             -
Tcp Syn Srcport less 1024    Disabled  Drop             -
DES-1210-52/ME:5#
```

To display DoS prevention information for Land Attack:

```
DES-1210-52/ME:5# show dos_prevention land_attack
Command: show dos_prevention land_attack

DosType                    State        Action
---------------------------  -----------   ---------------------
Land Attack                Enabled      Drop
DES-1210-52/ME:5#
```

enable dos_prevention trap_log

Purpose	Used to enable DoS prevention trap log.
Syntax	**enable dos_prevention trap_log**
Description	The **enable dos_prevention trap_log** command is used to enable DoS prevention trap log.
Parameters	None.
Restrictions	None.

Example usage:

To enable DoS prevention trap log on the Switch:

```
DES-1210-52/ME:5# enable dos_prevention trap_log
Command: enable dos_prevention trap_log

Success.

DES-1210-52/ME:5#
```

disable dos_prevention trap_log

Purpose	Used to disable DoS prevention trap log.
Syntax	**disable dos_prevention trap_log**
Description	The **disable dos_prevention trap_log** command is used to disable DoS prevention trap log.
Parameters	None.
Restrictions	None.

Example usage:

To disable DoS prevention trap log on the Switch:

```
DES-1210-52/ME:5# disable dos_prevention trap_log
Command: disable dos_prevention trap_log

Success.

DES-1210-52/ME:5#
```

11

PPPOE CIRCUIT ID INSERTION COMMANDS

PPPoE Circuit ID Insertion is used to produce the unique subscriber mapping capability that is possible on ATM networks between ATM-DSL local loop and the PPPoE server. The PPPoE server will use the inserted Circuit Identifier sub-tag of the received packet to provide AAA services (Authentication, Authorization and Accounting). Through this method, Ethernet networks can be as the alternative of the ATM networks.

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

Command	Parameter
config pppoe circuit_id _insertion state	[enable | disable]
config pppoe circuit_id_insertion ports	<portlist> [circuit_id [mac | ip | udf <string 32>] | state [enable | disable]]
show pppoe circuit_id_insertion	
show pppoe circuit_id_insertion ports	{<portlist>}

Each command is listed in detail, as follows:

config pppoe circuit_id_insertion state

Purpose	Used to enable or disable the PPPoE circuit identifier insertion.
Syntax	**config pppoe circuit_id_insertion state [enable | disable]**
Description	When PPPoE circuit identifier insertion is enabled, the system will insert the circuit ID tag to the received PPPoE discover and request packet if the tag is absent, and remove the circuit ID tag from the received PPPoE offer and session confirmation packet. The inserted circuit ID contains the following information: Client MAC address Device ID Port number By default, the Switch IP address is used as the device ID to encode the circuit ID option.
Parameters	*[enable | disable]* – Enables or disable PPPoE circuit ID insertion globally. The function is disabled by default.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To globally enable PPPoE circuit identifier insertion:

```
DES-1210-52/ME:5# config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable
```

```
Success.

DES-1210-52/ME:5#
```

config pppoe circuit_id_insertion ports

Purpose	Used to enable and disable PPPoE circuit identifier insertion on a per port basis and specify how to encode the circuit ID option.
Syntax	**config pppoe circuit_id_insertion ports <portlist> [circuit_id [mac | ip | udf <string 32>] | state [enable | disable]]**
Description	When the port's state and the global state are enabled, the system will insert the Circuit ID TAG to the received PPPoE discovery initiation and request packet if the TAG is absent, and remove the Circuit ID tag, inserted by the system, from the received PPPoE offer and session confirmation packet.
Parameters	*<portlist>* – Specifies a list of ports to be configured. The default settings are enabled for ID insertion per port, but disabled globally. *circuit_id* – Configures the device ID used for encoding of the circuit ID option. *mac* – Specifies that the Switch MAC address be used to encode the circuit ID option. *ip* – Specifies that the Switch IP address be used to encode the circuit ID option. *udf* – A user defined string to be used to encode the circuit ID option. The maximum length is 32. The default encoding for the device ID option is the Switch IP address. *state* – Specify to enable or disable PPPoE circuit ID insertion for the ports listed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable port 1~5 PPPoE circuit ID insertion function and use Host MAC:

```
DES-1210-52/ME:5# config pppoe circuit_id_insertion ports 1-5 circuit_id
mac state enable
Command: config pppoe circuit_id_insertion ports 1-5 circuit_id mac
state enable

Success.

DES-1210-52/ME:5#
```

show pppoe circuit_id_insertion

Purpose	Used to display the PPPoE circuit identifier insertion status for the Switch.
Syntax	**show pppoe circuit_id_insertion**
Description	The **show pppoe circuit_id_insertion** command is used to display

	the global state configuration of the PPPoE circuit ID insertion function.
Parameters	None.
Restrictions	None.

Example usage:

To view the global PPPoE ID insertion state:

```
DES-1210-52/ME:5# show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Status: Enabled

DES-1210-52/ME:5#
```

show pppoe circuit_id_insertion ports

Purpose	Used to display the PPPoE ID insertion configuration on a per port basis.
Syntax	**show pppoe circuit_id_insertion ports {<portlist>}**
Description	The **show pppoe circuit_id_insertion ports** command allows the user to view the configuration of PPPoE ID insertion for each port.
Parameters	*<portlist>* - Specifies which ports to display. If no ports are specified, all ports configuration will be listed.
Restrictions	None.

Example usage:

To view the PPPoE circuit ID configuration for ports 6 to 8:

```
DES-1210-52/ME:5# show pppoe circuit_id_insertion ports 6-8
Command: show pppoe circuit_id_insertion ports 6-8

Port State    PPPoE Tags
---- -------- --------------------------------------------
6    Enabled  Circuit ID : Switch MAC
              Remote ID  : Default

7    Enabled  Circuit ID : Switch MAC
              Remote ID  : Default

8    Enabled  Circuit ID : Switch MAC
              Remote ID  : Default

DES-1210-52/ME:5#
```

12

DHCP SERVER SCREENING COMMANDS

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

Due to this function allow you not only to restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more than one DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

When DHCP Server Screening function is enabled, all DHCP Server packets will be filtere from a specif ic port. Also, you are allow to create entries for specific Server IP address an d Client MAC address bi nding by por t-based. Be aware th a tthe DHCP Ser ver Screen ing f uncti n must b e enabled first On ce all sett ng is do ne, all DHC P Serve packe s wi ll be filtered fro m a speci fic port e cep t those tha meet th e Se ver IP Ad dres s and Cli ent M AC Addres s binding .

Command	Parameter
config filter dhcp_server	[add permit server_ip <ipaddr> { client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> { client_mac <macaddr> } {ports <portlist> state [enable | disable]}
config filter dhcp_server	illegal_server_log_suppress_duration [<1min | 5min | 30min>]
config filter dhcp_server log state	[enable | disable]
show filter dhcp_server	
show dhcp_server screening	
create filter dhcpv6_server permit_entry	<ipv6addr> ports [<portlist> | all]
delete filter dhcpv6_server permit_entry	<ipv6addr>
config filter dhcpv6_server ports	<portlist> state [enable | disable]
config filter dhcpv6_server log state	[enable | disable]
show filter dhcpv6_server	

Each command is listed in detail, as follows:

config filter dhcp_server	
Purpose	DHCP server packets except those that have been IP/client MAC bound will be filtered. This command is used to configure the state of the function for filtering of DHCP server packet and to add/delete the

	DHCP server/client binding entry.
Syntax	**config filter dhcp_server [add permit server_ip <ipaddr> { client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> { client_mac <macaddr> } {ports <portlist> state [enable | disable]}**
Description	The **config filter dhcp_server** command has two purposes: To filter all DHCP server packets on the specified port(s) and to allow some DHCP server packets to forwarded if they are on the pre-defined server IP address/MAC address binding list. Thus the DHCP server can be restricted to service a specified DHCP client. This is useful when there are two or more DHCP servers present on f network.
Parameters	<*ipaddr*> – The IP address of the DHCP server to be filtered *client_mac <macaddr>* – The MAC address of the DHCP client. *ports <portlist>* – The port number to which the DHCP filter will be applied. *state* – Enable/Disable the DHCP filter state.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To add an entry from the DHCP server/client filter list in the Switch’s database:

```
DES-1210-52/ME:5# config filter dhcp_server add permit server_ip
10.1.1.1 client_mac 00-00-00-00-00-01 ports 6-8
Command: config filter dhcp_server add permit server_ip 10.1.1.1
client_mac 00-00-00-00-00-01 ports 6-8



Success.
DES-1210-52/ME:5#
```

config filter dhcp_server	
Purpose	DHCP.
Syntax	**config filter dhcp_server illegal_server_log_suppress_duration [<1min | 5min | 30min>]**
Description	The **config filter dhcp_server** command.
Parameters	<*1min* | *5min* | *30min*> – Specify the duration time.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the illegal server log suppress duration time to 5 minutes:

```
DES-1210-52/ME:5# config filter dhcp_server illegal_server_log_suppress_duration
5min
Command: config filter dhcp_server illegal_server_log_suppress_duration 5min

Success.

DES-1210-52/ME:5#
```

config filter dhcp_server log state

Purpose	To enable or disable the DHCP server log on the Switch.
Syntax	**config filter dhcp_server log state [enable | disable]**
Description	The **config filter dhcp_server log state** command is used to enable or disable the Filter DHCP server log state.
Parameters	*state [enable | disable]* – Specifies that the log for the Filter DHCP server will be enabled or disabled.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the Filter DHCP Server log state:

```
DES-1210-52/ME:5# config filter dhcp_server log state enable
Command: config filter dhcp_server log state enable



Success.
DES-1210-52/ME:5#
```

show filter dhcp_server

Purpose	Used to display current DHCP server/client filter list created on the switch.
Syntax	**show filter dhcp_server**
Description	The **show filter dhcp_server** command is used to display DHCP server/client filter list created on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server filter list created on the switch:

```
DES-1210-52/ME:5# show filter dhcp_server
Command: show filter dhcp_server

Enabled ports :
Illegal Server Log Suppress Duration : 5 Minutes

Permit DHCP Server/Client Table:
Server IP Address  Client MAC Address Ports
-------------------------- ---------------------------- ----------------
10.1.1.1               00-00-00-00-00-01     6-8
DES-1210-52/ME:5#
```

show dhcp_server screening

Purpose	Used to display current DHCP server screening information on the switch.
Syntax	**show dhcp_server screening**

Description	The **show dhcp_server screening** command is used to display current DHCP server screening information on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server screening information on the switch:

```
DES-1210-52/ME:5# show dhcp_server screening
Command: show dhcp_server screening

Illegal Server Log Suppress Duration : 5 Minutes

DHCP server screening :

Port  Admin 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
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

create filter dhcpv6_server permit_entry

Purpose	DHCPv6 server packets except those that have been IP/client MAC bound will be filtered. This command is used to create a permit entry. The specific DHCPv6 server packets, with the source IPv6 address, will be forwarded on t he specified ports.
Syntax	**create filter dhcpv6_server permit_entry <ipv6addr> ports [<portlist> | all]**
Description	The **create filter dhcpv6_server permit_entry** command is used to create a permit entry. The specific DHCPv6 server packets, with the source IPv6 address, will be forwarded on the specified ports.
Parameters	*<ipv6addr>* – The IPv6 address of the DHCPv6 server to be filtered. *ports [<portlist>* | *all]* – The ports or all ports to which the DHCPv6 filter will be applied.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an entry from the DHCPv6 server filter list in the Switch's database:

```
DES-1210-52/ME:5# create filter dhcpv6_server permit_entry 3000::1 ports 1-3
Command: create filter dhcpv6_server permit_entry 3000::1 ports 1-3


Success.
DES-1210-52/ME:5#
```

delete filter dhcpv6_server permit_entry

Purpose	To delete a filter DHCPv6 server permit entry.
Syntax	**delete filter dhcpv6_server permit_entry <ipv6addr>**
Description	The **delete filter dhcpv6_server permit_entry** command is used to delete a filter DHCPv6 server permit entry.
Parameters	*<ipv6addr>* – The IPv6 address of the DHCPv6 server to be removed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete permit entry from the filter DHCPv6 server forward list:

```
DES-1210-52/ME:5# delete filter dhcpv6_server permit_entry 3000::1
Command: delete filter dhcpv6_server permit_entry 3000::1


Success.
DES-1210-52/ME:5#
```

config filter dhcpv6_server ports

Purpose	To configure the state of filter DHCPv6 server packets on the Switch.
Syntax	**config filter dhcpv6_server ports <portlist> state [enable | disable]**
Description	The **config filter dhcpv6_server ports** command is used to configure the state of filter DHCPv6 server packets on the Switch. The filter DHCPv6 server function is used to filter the DHCPv6 server packets on the specific ports and receive the trust packets from the specific source. This feature can be proteted network usable when a malicious host sends the DHCPv6 server packets.
Parameters	*<portlist>* – Specifies the ports to be configured. *state [enable | disable]* – Specifies whether the port's filter DHCPv6 server function is enabled or disabled.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the filter DHCPv6 server state to be enabled for ports 3-5:

```
DES-1210-52/ME:5# config filter dhcpv6_server ports 3-5 state enable
Command: config filter dhcpv6_server ports 3-5 state enable
```

```


Success.
DES-1210-52/ME:5#
```

config filter dhcpv6_server log state

Purpose	To enable or disable the DHCPv6 server log on the Switch.
Syntax	**config filter dhcpv6_server log state [enable | disable]**
Description	The **config filter dhcpv6_server log state** command is used to enable or disable the Filter DHCPv6 server log state.
Parameters	*state [enable* | *disable]* – Specifies that the log for the Filter DHCPv6 server will be enabled or disabled.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the Filter DHCPv6 Server log state:

```
DES-1210-52/ME:5# config filter dhcpv6_server log state enable
Command: config filter dhcpv6_server log state enable


Success.
DES-1210-52/ME:5#
```

show filter dhcpv6_server

Purpose	Used to display the filter DHCPv6 server information on the switch.
Syntax	**show filter dhcpv6_server**
Description	The **show filter dhcpv6_server** command is used to display the filter DHCPv6 server information on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the filter DHCPv6 server information on the switch:

```
DES-1210-52/ME:5# show filter dhcpv6_server
Command: show filter dhcpv6_server

Enabled ports : 2-5
DHCPv6 Filter Syslog State : Enable


Success.
DES-1210-52/ME:5#
```

13

IP-MAC-PORT 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-port 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-port binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC-port binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the Switch, the maximum value for the IP-MAC-port binding ARP mode is 500. 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.

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

Command	Parameter
create address_binding ip_mac	[ipaddress <ipaddr> | ipv6address <ipv6addr>] mac_address <macaddr> port <port 1-52>
config address_binding ip_mac ports	[<portlist> | all] {state [disable | enable] | ip_inspection [disable | enable] | arp_inspection [loose | strict] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable]}
config address_binding ip_mac log	[all | disable | ipv4 | ipv6]
show address_binding ip_mac log	
config address_binding auto_scan	from_ip <ipaddr> to_ip <ipaddr>
config address_binding auto_scan ipv6address	from_ip <ipv6addr> to_ip <ipv6addr>
delete address_binding	[ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr> | all] | blocked [all | vlan_name <string 32> mac_address <macaddr>]]
show address_binding	{[ip_mac [all | {ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr>}] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <port 1-52>] | ports]}
show address_binding auto_scan list	
enable address_binding dhcp_snoop	ports [<portlist> | all]
disable address_binding dhcp_snoop	ports [<portlist> | all]
config address_binding dhcp_snoop max_entry ports	[<portlist> | all] limit [<int 1-10> | no_limit] {IPv6}

Command	Parameter
show address_binding dhcp_snoop	[binding_entry | max_entry | vlan_list] ports <portlist>
enable address_binding dhcp_pd_snoop	
disable address_binding dhcp_pd_snoop	
show address_binding dhcp_pd_snoop	{binding_entry | ports <portlist>}
config address_binding vlan	{<vidlist>} vlan_mode state [enable | disable]
enable address_binding roaming	
disable address_binding roaming	
show address_binding roaming	
clear address_binding dhcp_snoop binding_entry ports	[<portlist> | all] {all | ipv6}

Each command is listed in detail, as follows:

create address_binding ip_mac	
Purpose	Used to create an IP-MAC-port binding entry.
Syntax	**create address_binding ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr>] mac_address <macaddr> port <port 1-52>**
Description	The **create address_binding ip_mac ipaddress** command is used to create an IP-MAC-port binding entry.
Parameters	*ipaddress <ipaddr>* – The IPv4 address of the device where the IP-MAC-port binding is made. *Ipv6address <ipv6addr>* – The IPv4v6 address of the device where the IP-MAC-port binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC-port binding is made. *<port 1-52>* – Specifies a port to be configured for address binding.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DES-1210-52/ME:5# create address_binding ip_mac ipaddress 10.0.0.21
mac_address 00-00-00-00-01-02 port 3
```

```
Command: create address_binding ip_mac ipaddress 10.0.0.21
mac_address 00-00-00-00-01-02 port 3

Success.
DES-1210-52/ME:5#
```

config address_binding ip_mac ports

Purpose	Used to configure an IP-MAC-port binding state to enable or disable for specified ports.
Syntax	**config address_binding ip_mac ports [<portlist> | all] {state [disable | enable] | ip_inspection [disable | enable] | arp_inspection [loose | strict] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable]}**
Description	The **config address_binding ip_mac ports** command is used to configure the IP-MAC-port binding state to enable or disable for specified ports.
Parameters	*<portlist>* − Specifies a port or range of ports. *all* – Specifies all ports on the switch. *[enable* | *disable]* – Enables or disables the specified range of ports for state, IP-inspection, allow_zeroip and forward_dhcppkt. *arp_inspection [loose* | *strict]* – Specifies to check the ARP inspection to be loose or stict for the specified ports.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-1210-52/ME:5# config address_binding ip_mac ports 3 state disable
arp_inspection loose ip_inspection disable
Command: config address_binding ip_mac ports 3 state disable
arp_inspection loose ip_inspection disable

Success.
DES-1210-52/ME:5#
```

config address_binding ip_mac log

Purpose	Used to configure an IP-MAC-port binding state to enable or disable for specified log.
Syntax	**config address_binding ip_mac log [all | disable | ipv4 | ipv6]**
Description	The **config address_binding ip_mac log** command is used to configure the IP-MAC-port binding state to enable or disable for specified log.
Parameters	*[all* | *disable* | *ipv4* | *ipv6]* − Specifies a specified log or all log to be configured.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-1210-52/ME:5# config address_binding ip_mac log all
```

```
Command: config address_binding ip_mac log all

Success.
DES-1210-52/ME:5#
```

show address_binding ip_mac log

Purpose	Used to display an IP-MAC-port binding IP MAC log information.
Syntax	**show address_binding ip_mac log**
Description	The **show address_binding ip_mac log** command is used to display an IP-MAC-port binding IP MAC log information.
Parameters	None.
Restrictions	None.

Example usage:

To display address binding IP MAC log information on the Switch:

```
DGS-1210-28P/ME:5# show address_binding ip_mac log
Command: show address_binding ip_mac log

Log status: IPv4
DGS-1210-28P/ME:5#
```

config address_binding auto_scan

Purpose	Used to configure an IP-MAC-port binding auto scan for specified IP addresses.
Syntax	**config address_binding auto_scan from_ip <ipaddr> to_ip <ipaddr>**
Description	The **config address_binding auto_scan** command is used to configure the IP-MAC-port binding auto scan for specified IP addresses.
Parameters	*<ipaddr>* − Specifies a range of IP addresses for address binding auto scan on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding auto scan on the Switch:

```
DES-1210-52/ME:5# config address_binding auto_scan from_ip 10.0.0.10
to_ip 10.0.0.12
Command: config address_binding auto_scan from_ip 10.0.0.10 to_ip
10.0.0.12

Success.
DES-1210-52/ME:5#
```

config address_binding auto_scan ipv6address

Purpose	Used to configure an IP-MAC-port binding auto scan for specified

	IPv6 addresses.
Syntax	**config address_binding auto_scan ipv6address from_ip <ipv6addr> to_ip <ipv6addr>**
Description	The **config address_binding auto_scan** command is used to configure the IP-MAC-port binding auto scan for specified IPv6 addresses.
Parameters	*<ipv6addr>* − Specifies a range of IPv6 addresses for address binding auto scan on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding auto scan on the Switch:

```
DES-1210-52/ME:5# config address_binding auto_scan ipv6address from_ip
3000::1 to_ip 3000::3
Command: config address_binding auto_scan ipv6address from_ip 3000::1
to_ip 3000::3

Success.
DES-1210-52/ME:5#
```

delete address_binding

Purpose	Used to delete IP-MAC-port binding entries.
Syntax	**delete address_binding [ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr> | all] | blocked [all | vlan_name <string 32> mac_address <macaddr>]**
Description	The **delete address_binding** command is used to delete IP-MAC-port 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	*ipaddress <ipaddr>* – The IPv4 address of the device where the IP-MAC-port binding is made. *iv6paddress <ipv6addr>* – The IPv6 address of the device where the IP-MAC-port binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC-port binding is made. *vlan_name <string 32>* – 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-port binding all specifies all the IP-MAC-port binding entries; for blocked address binding entries all specifies all the blocked VLANs and their bound physical sddresses.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete all address binding entries on the Switch:

```
DES-1210-52/ME:5# delete address_binding ip_mac all
Command: delete address_binding ip_mac all

Success.
DES-1210-52/ME:5#
```

show address_binding

Purpose	Used to display IP-MAC-port binding entries.
Syntax	**show address_binding {[ip_mac [all | {ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr>}] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <port 1-52>] | ports]}**
Description	This **show address_binding** command is used to display IP-MAC-port binding entries. Four 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 the device.
Parameters	*ip_mac* – The database the user creates for address binding. *all* – For IP MAC binding all specifies all the IP-MAC-port binding entries; for blocked address binding entries all specifies all the blocked VLANs and their bound physical addresses. *blocked* – The address database that the system auto learns and blocks. *ipaddress <ipaddr>* – The IPv4 address of the device where the IP-MAC-port binding is made. *ipv6address <ipv6addr>* – The IPv6 address of the device where the IP-MAC-port binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC-port binding is made. *vlan_name <string 32>* – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN. *port <port 1-52>* – Specifies a port to be displayed for the address binding on the Switch.
Restrictions	None.

Example usage:

To display address binding entries on the Switch:

```
DES-1210-52/ME:5# show address_binding ip_mac all
Command: show address_binding ip_mac all

IP Address     MAC Address        Port
---------------  --------------------   ----
10.0.0.21        00-00-00-00-01-02   3

DES-1210-52/ME:5#
```

show address_binding auto_scan list

Purpose	Used to display IP-MAC-port binding entries.
Syntax	**show address_binding auto_scan list**
Description	This **show address_binding auto_scan list** command is used to display auto scan list of address binding on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the auto scan list of address binding on the Switch:

```
DES-1210-52/ME:5# show address_binding auto_scan list
Command: show address_binding auto_scan list

VLAN IP Address     MAC Address      Port Bound
--------- -----------------  ---------------------    ------  -----------


Total Entries : 0
DES-1210-52/ME:5#
```

enable address_binding dhcp_snoop

Purpose	Used to enable address binding DHCP Snooping.
Syntax	**enable address_binding dhcp_snoop ports [<portlist> | all]**
Description	This **enable address_binding dhcp_snoop** command is used to enable IP-MAC-port binding DHCP snooping entries.
Parameters	*[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be enabled of the address binding DHCP snooping on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the DHCP snooping of address binding for port 3~5 on the Switch:

```
DES-1210-52/ME:5# enable address_binding dhcp_snoop ports 3-5
Command: enable address_binding dhcp_snoop ports 3-5

Success.
DES-1210-52/ME:5#
```

disable address_binding dhcp_snoop

Purpose	Used to disable address binding DHCP Snooping.
Syntax	**disable address_binding dhcp_snoop ports [<portlist> | all]**
Description	This **disable address_binding dhcp_snoop** command is used to disable IP-MAC-port binding DHCP snooping entries.
Parameters	*[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be enabled of the address binding DHCP snooping on the Switch.

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

Example usage:

To disable the DHCP snooping of address binding for port 3~5 on the Switch:

```
DES-1210-52/ME:5# disable address_binding dhcp_snoop ports 4
Command: disable address_binding dhcp_snoop ports 4

Success.
DES-1210-52/ME:5#
```

config address_binding dhcp_snoop max_entry ports

Purpose	Used to specify the maximum number of entries which can be dynamically learned (DHCP snooping) by the specified ports.
Syntax	**config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<int 1-10> | no_limit] {IPv6}**
Description	This **config address_binding dhcp_snoop max_entry ports** command is used to specify the maximum number of DHCP snooping entries on specified ports. By default, the per-port maximum entry has no limit.
Parameters	*[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be configured of the address binding DHCP snooping on the Switch. *[<int 1-10>* | *no_limit]* – Specifies the limit for max entry number. *{IPv6}* – Specifies the IPv6 address used for this configuration.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the DHCP snooping of address binding for port 1 on the Switch:

```
DES-1210-52/ME:5# config address_binding dhcp_snoop max_entry
ports 1 limit 1
Command: config address_binding dhcp_snoop max_entry ports 1
limit 1

Success.
DES-1210-52/ME:5#
```

show address_binding dhcp_snoop

Purpose	Used to display DHCP snoop of IP-MAC-port binding.
Syntax	**show address_binding dhcp_snoop [binding_entry | max_entry | vlan_list] port <portlist>**
Description	This **show address_binding dhcp_snoop** command is used to display DHCP snoop of IP-MAC-port binding entries. Two different kinds of information can be viewed. They are binding entry and max entry. *[binding_entry* | *max_entry* | *vlan_list]* – Address binding entries can be viewed by entering the physical and IP addresses of the device. *port* – The number of enabled ports on the device to be displayed.
Parameters	*[binding_entry* | *max_entry* | *vlan_list]* – Specifies address binding entries can be viewed

	port <portlist> – Specifies the ports on the device to be displayed.
Restrictions	None.

Example usage:

To display DHCP snoop of address binding max entries of port 1~5 on the Switch:

```
DES-1210-52/ME:5# show address_binding dhcp_snoop max_entry
ports 1-5
Command: show address_binding dhcp_snoop max_entry ports 1-5

Port  Max Entry  Max IPv6 Entry
----  ---------- ----------------
1     No Limit   No Limit
2     No Limit   No Limit
3     No Limit   No Limit
4     No Limit   No Limit
5     No Limit   No Limit
DES-1210-52/ME:5#
```

enable address_binding dhcp_pd_snoop

Purpose	Used to enable address binding DHCPv6 PD Snooping.
Syntax	**enable address_binding dhcp_pd_snoop**
Description	This **enable address_binding dhcp_pd_snoop** command is used to enable IP-MAC-port binding DHCPv6 PD snooping.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable address binding DHCPv6 PD Snooping on the Switch:

```
DES-1210-52/ME:5# enable address_binding dhcp_pd_snoop
Command: enable address_binding dhcp_pd_snoop

Success.
DES-1210-52/ME:5#
```

disable address_binding dhcp_pd_snoop

Purpose	Used to disable address binding DHCPv6 PD Snooping.
Syntax	**disable address_binding dhcp_pd_snoop**
Description	This **disable address_binding dhcp_pd_snoop** command is used to disable IP-MAC-port binding DHCPv6 PD snooping.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable address binding DHCPv6 PD Snooping on the Switch:

```
DES-1210-52/ME:5# disable address_binding dhcp_pd_snoop
```

```
Command: disable address_binding dhcp_pd_snoop

Success.
DES-1210-52/ME:5#
```

show address_binding dhcp_pd_snoop

Purpose	Used to display address binding DHCPv6 PD Snooping.
Syntax	**show address_binding dhcp_pd_snoop {binding_entry | ports <portlist>}**
Description	This **show address_binding dhcp_pd_snoop** command is used to display IP-MAC-port binding DHCPv6 PD snooping.
Parameters	None.
Restrictions	None.

Example usage:

To display address binding DHCPv6 PD Snooping on the Switch:

```
DES-1210-52/ME:5# show address_binding dhcp_pd_snoop binding_entry
Command: show address_binding dhcp_pd_snoop binding_entry

IP Address                           Port Lease  Remain
------------------------------------ ------- ---------- ------------



Total Entries  : 0

DES-1210-52/ME:5#
```

enable address_binding roaming

Purpose	Used to enable address binding roaming.
Syntax	**enable address_binding roaming**
Description	This **enable address_binding roaming** command is used to enable IP-MAC-port binding roaming.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the roaming of address binding on the Switch:

```
DGS-1210-28/ME:5# enable address_binding roaming
Command: enable address_binding roaming

Success.
DES-1210-52/ME:5#
```

disable address_binding roaming

Purpose	Used to disable address binding roaming.
Syntax	**disable address_binding roaming**
Description	This **disable address_binding roaming** command is used to disable IP-MAC-port binding roaming.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable the roaming of address binding on the Switch:

```
DGS-1210-28/ME:5# disable address_binding roaming
Command: disable address_binding roaming

Success.
DES-1210-52/ME:5#
```

show address_binding roaming

Purpose	Used to display DHCP snoop of IP-MAC-port binding lroaming information.
Syntax	**show address_binding roaming**
Description	This **show address_binding roaming** command is used to display DHCP snoop of IP-MAC-port binding roaming information.
Parameters	None.
Restrictions	None.

Example usage:

To display DHCP snoop of address binding roaming information on the Switch:

```
DGS-1210-28/ME:5# show address_binding roaming
Command: show address_binding roaming

Roaming state is enabled.
DES-1210-52/ME:5#
```

clear address_binding dhcp_snoop binding_entry ports

Purpose	Used to clear the DHCP snooping entries learned for the specified ports.
Syntax	**clear address_binding dhcp_snoop binding_entry ports [<portlist> | all] {all | ipv6}**
Description	This **clear address_binding dhcp_snoop binding_entry ports** command is used to clear the DHCP snooping entries learned for the specified ports.
Parameters	*[<portlist> | all]* – Specifies a range of ports or all ports to be configured. *all* - Specifies that all entries will be cleared. *ipv6* - Specifies that IPv6 entries will be cleared.

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

Example usage:

To clear DHCP IPv4 snooping entries on ports 1-3:

```
DES-1210-52/ME:5# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.
DES-1210-52/ME:5#
```

14

NETWORK MANAGEMENT (SNMP) COMMANDS

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

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

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

Command	Parameter
create snmp user	<username 32> <groupname 32> [v1 | v2c | v3 [MD5 <auth_password 32> | SHA <auth_password 32> | none] [DES <priv_password 32> | none]]
delete snmp user	<username 32> [v1 | v2c | v3]
show snmp user	
create snmp view	<view_name 32> <oid 32> <oid_mask 32 view_type [included | excluded]
delete snmp view	<view_name 32> <oid 32>
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> <username 32>
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID 64>
show snmp engineID	
create snmp group	<groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]{notify_view <view_name 32>}] {read_view <view_name 32> | write_view <view_name 32>}
delete snmp group	<groupname 32> [v1 | v2c | v3] [auth_nopriv | auth_priv | noauth_priv]
show snmp global state	

Command	Parameter
show snmp groups	
create snmp host	<ipaddr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]
delete snmp host	<ipaddr>
show snmp host	{<ipaddr>}
create snmp v6host	<ip6_addr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]
delete snmp v6host	<ipv6_addr>
show snmp v6host	<ipv6_addr>
enable trusted_host	
disable trusted_host	
create trusted_host	[<ipaddr> | network <network_address> | <ipv6_addr> | ipv6_prefix <ipv6networkaddr>]
show trusted_host	
delete trusted_host	[<ipaddr> | network <network_address> | <ipv6_addr> | ipv6_prefix <ipv6networkaddr> | all]
enable snmp traps	
disable snmp traps	
enable snmp authenticate trap	
disable snmp authenticate trap	
show snmp traps	
enable snmp linkchange_traps	
disable snmp linkchange_traps	
config snmp linkchange_traps ports	[<portlist> | all] [enable | disable]
show snmp traps linkchange_traps	
config snmp system_contact	<string 128>
config snmp system_location	<string 128>
config snmp system_name	<string 128>
config snmp warmstart_traps	[enable | disable]
config snmp	[enable | disable]

Command	Parameter
coldstart_traps	
enable snmp	
disable snmp	
enable snmp DHCP_screening traps	
diable snmp DHCP_screening traps	
enable snmp DHCPv6_screening traps	
diable snmp DHCPv6_screening traps	
enable snmp IMPB_violation traps	
disable snmp IMPB_violation traps	
enable snmp firmware_upgrade_state traps	
disable snmp firmware_upgrade_state traps	
enable snmp LBD traps	
disable snmp LBD traps	
enable snmp port_security_violation traps	
disable snmp port_security_violation traps	
enable snmp rstpport_state_change traps	
disable snmp rstpport_state_change traps	
enable snmp system_device_bootup traps	
disable snmp system_device_bootup traps	
enable snmp twistedpair_port_link	

Command	Parameter
traps	
disable snmp twistedpair_port_link traps	
enable snmp duplicate_IP_detected traps	
disable snmp duplicate_IP_detected traps	

Each command is listed in detail, as follows:

create snmp user	
Purpose	To create a new SNMP user and add the user to an SNMP group.
Syntax	**create snmp user <username 32> <groupname 32> [v1 | v2c | v3 [MD5 <auth_password 32> | SHA <auth_password 32> | none] [DES <priv_password 32> | none]]**
Description	The **create snmp user** command creates a new SNMP user and adds the user to an existing SNMP group.
Parameters	*<username 32>* − The new SNMP username, up to 32 alphanumeric characters. *<groupname 32>* − The SNMP groupname the new SNMP user is associated with, up to 32 alphanumeric characters. *auth* - The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are: • *MD5* − Specifies that the HMAC-MD5-96 authentication level to be used. md5 may be utilized by entering one of the following: • *<auth password 32>* - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host. • *SHA* − Specifies that the HMAC-SHA-96 authentication level will be used. • *<priv_password 32>* - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host. • *DES* − Specifies that the DES authentication level will be used.
Restrictions	Only administrator, operate or power user-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DES-1210-52/ME:5# create snmp user dlink sw22 v3 MD5 1234 DES 2233
Command: create snmp user dlink sw22 v3 MD5 1234 DES 2233
```

```

Success.
DES-1210-52/ME:5#
```

delete snmp user

Purpose	To remove an SNMP user from an SNMP group and also to delete the associated SNMP group.
Syntax	**delete snmp user <username 32> [v1 | v2c | v3]**
Description	The **delete snmp user** command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	*<username 32>* − A string of up to 32 alphanumeric characters that identifies the SNMP user to be deleted.
Restrictions	Only administrator, operate or power user-level users can issue this command.

Example usage:

To delete an SNMP user on the Switch:

```
DES-1210-52/ME:5# delete snmp user dlink v3
Command: delete snmp user dlink v3



Success.
DES-1210-52/ME:5#
```

show snmp user

Purpose	To display information about each SNMP username in the SNMP group username table.
Syntax	**show snmp user**
Description	The **show snmp user** command displays information about each SNMP username in the SNMP group username table.
Parameters	None.
Restrictions	None.

Example usage:

To display the SNMP users currently configured on the Switch:

```
DES-1210-52/ME:5# show snmp user
Command: show snmp user

Username   Group Name   SNMP Version   Auth-Protocol    PrivProtocol
---------  -----------  -----------    -------------    ----------


ReadOnly   ReadOnly        V1             None             None
ReadOnly   ReadOnly        V2             None             None
ReadWrite  ReadWrite       V1             None             None
ReadWrite  ReadWrite       V2             None             None

```

```
Total Entries: 4

DES-1210-52/ME:5#
```

create snmp view

Purpose	To assign views to community strings to limit which MIB objects an SNMP manager can access.
Syntax	**create snmp view <view_name 32> <oid 32> <oid_mask 32 view_type [included | excluded]**
Description	The **create snmp view** command assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	<*view_name 32*> − A string of up to 30 alphanumeric characters that identifies the SNMP view to be created. <*oid 32*> − The object ID that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager. <*oid_mask 32*> − The object ID mask that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager. *included* − Includes this object in the list of objects that an SNMP manager can access. *excluded* − Excludes this object from the list of objects that an SNMP manager can access.
Restrictions	Only administrator, operate or power user-level users can issue this command.

Example usage:

To create an SNMP view:

```
DES-1210-52/ME:5# create snmp view dlink 1.3.6 1.1.1 view_type excluded
Command: create snmp view dlink 1.3.6 1.1.1 view_type excluded



Success.
DES-1210-52/ME:5#
```

delete snmp view

Purpose	To remove an SNMP view entry previously created on the Switch.
Syntax	**delete snmp view <view_name 32> <oid 32>**
Description	The **delete snmp view** command removes an SNMP view previously created on the Switch.
Parameters	<*view_name 32*> − A string of up to 32 alphanumeric characters that identifies the SNMP view to be deleted. <*oid 32*> − The object ID that identifies an object tree (MIB tree) that is deleted from the Switch.
Restrictions	Only administrator, operate or power user-level users can issue this command.

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DES-1210-52/ME:5# delete snmp view dlink 1.3.6
Command: delete snmp view dlink 1.3.6

Success.

DES-1210-52/ME:5#
```

show snmp view

Purpose	To display an SNMP view previously created on the Switch.
Syntax	**show snmp view {<view_name 32>}**
Description	The **show snmp view** command displays an SNMP view previously created on the Switch.
Parameters	<*view_name 32*> − A string of up to 30 alphanumeric characters that identifies the SNMP view to be displayed.
Restrictions	None.

Example usage:

To display SNMP view configuration:

```
DES-1210-52/ME:5# show snmp view
Command: show snmp view

SNMP View Table Configuration
View Name      Subtree OID           OID Mask          View Type
--------------  ---------------------  ---------------------  ---------------
dlink           1.2.3.4               1.1.1.1            Excluded
ReadWrite       1                     1                  Included

Total Entries: 2

DES-1210-52/ME:5#
```

create snmp community

Purpose	To create an SNMP community string to define the relationship between the SNMP manager and an SNMP agent.
Syntax	**create snmp community <community_string 32> <username 32>**
Description	The **create snmp community** command creates an SNMP community string and assigns access-limiting characteristics to this community string. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string: An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent. A MIB view that defines the subset of all MIB objects to be accessible to the SNMP community.

	Read/write or read-only level permission for the MIB objects accessible to the SNMP community.
Parameters	*<community_string 32>* − A string of up to 32 alphanumeric characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch’s SNMP agent. *<username 32>* − A string of up to 32 alphanumeric characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only administrator, operate or power user-level users can issue this command.

Example usage:

To create the SNMP community string ‘dlink:’

```
DES-1210-52/ME:5# create snmp community dlinkgroup dlink
Command: create snmp community dlinkgroup dlink

Success.
DES-1210-52/ME:5#
```

delete snmp community

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

Example usage:

To delete the SNMP community string ‘dlink’:

```
DES-1210-52/ME:5# delete snmp community dlink
Command: delete snmp community dlink


Success.
DES-1210-52/ME:5#
```

show snmp community

Purpose	To display SNMP community strings configured on the Switch.
Syntax	**show snmp community {<community_string 32>}**
Description	The **show snmp community** command displays SNMP community strings that are configured on the Switch.
Parameters	*<community_string 32>* − A string of up to 20 alphanumeric

	characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently entered SNMP community strings:

```
DES-1210-52/ME:5# show snmp community
Command: show snmp community

SNMP Community Table
(Maximum Entries : 10)

Community Name       User Name
-----------------------     ----------------
public                   ReadOnly
private                  ReadWrite

Total Entries: 2

DES-1210-52/ME:5#
```

config snmp engineID

Purpose	To configure a name for the SNMP engine on the Switch.
Syntax	**config snmp engineID <snmp_engineID 64>**
Description	The **config snmp engineID** command configures a name for the SNMP engine on the Switch.
Parameters	*<snmp_engineID 64>* − A string, of between 10 and 64 alphanumeric characters, to be used to identify the SNMP engine on the Switch.
Restrictions	Only administrator, operate or power user-level users can issue this command.

Example usage:

To give the SNMP agent on the Switch:

```
DES-1210-52/ME:5# config snmp engineID 12345678900
Command: config snmp engineID 12345678900

Success.
DES-1210-52/ME:5#
```

show snmp engineID

Purpose	To display the identification of the SNMP engine on the Switch.
Syntax	**show snmp engineID**
Description	The **show snmp engineID** command displays the identification of the SNMP engine on the Switch.

Parameters	None.
Restrictions	None.

Example usage:

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

```
DES-1210-52/ME:5# show snmp engineID
Command: show snmp engineID


Default SNMP Engine ID : 4445532d313231

SNMP Engine ID        : 012345678900


DES-1210-52/ME:5#
```

create snmp group

Purpose	To create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	**create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]{notify_view <view_name 32>}] {read_view <view_name 32> | write_view <view_name 32>}**
Description	The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	*<groupname 32>* − A name of up to 30 alphanumeric characters that identifies the SNMP group the new SNMP user is to be associated with. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − Ensures that packets have not been tampered with during transit. • Authentication − Determines if an SNMP message is from a valid source. • Encryption − Scrambles the contents of messages to prevent it from being viewed by an unauthorized source. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no

	encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. • <*view_name 32*> − A string of up to 32 objects that a remote SNMP manager is allowed to access on the Switch. *write_view* – Specifies that the SNMP group being created has write privileges. • <*view_name 32* identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. *notify_view* − Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. • <*view_name 32*> − A string of up to 32 alphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only administrator, operate or power user-level users can issue this command.

Example usage:

T o create an SNMP group named 'sg1:

```
DES-1210-52/ME:5# create snmp group sg1 v1 notify_view
sg1
Command: create snmp group sg1 v1 notify_view sg1



Success.
DES-1210-52/ME:5#
```

delete snmp group

Purpose	To remove an SNMP group from the Switch.
Syntax	**delete snmp group <groupname 32> [v1 | v2c | v3 [auth_priv | noauth_nopriv]]**
Description	The **delete snmp group** command removes an SNMP group from the Switch.
Parameters	<*groupname 32*> − A string of that identifies the SNMP group the new SNMP user will be associated with. Up to 32 alphanumeric characters.
Restrictions	Only administrator, operate or power user-level users can issue this command.

Example usage:

To delete the SNMP group named 'sg1':

```
DES-1210-52/ME:5# delete snmp group sg1 v1
Command: delete snmp group sg1 v1
```

```
Success.
DES-1210-52/ME:5#
```

show snmp global state

Purpose	To display the global state of SNMP currently configured on the Switch.
Syntax	**show snmp global state**
Description	The **show snmp global state** command displays the global state of SNMP groups currently configured on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the currently configured SNMP global state on the Switch:

```
DES-1210-52/ME:5# show snmp global state
Command: show snmp global state


SNMP Global State : Enable


DES-1210-52/ME:5#
```

show snmp groups

Purpose	To display the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Syntax	**show snmp groups**
Description	The **show snmp groups** command displays the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Parameters	None.
Restrictions	None.

Example usage:

To display the currently configured SNMP groups on the Switch:

```
DES-1210-52/ME:5# show snmp groups
Command: show snmp groups

SNMP Group Table

Group Name  Read View  Write View  Notify View  Security Model  Security Level
----------------- ------------- --------------- -------------- --------------------- ----------------
sg1          df          df          d             v3             AuthPriv
ReadOnly   ReadWrite   ---          ReadWrite   v1             NoAuthNoPriv
ReadOnly   ReadWrite   ---          ReadWrite   v2c            NoAuthNoPriv
ReadWrite  ReadWrite   ReadWrite  ReadWrite   v1             NoAuthNoPriv
ReadWrite  ReadWrite   ReadWrite  ReadWrite   v2c            NoAuthNoPriv

Total Entries: 5

DES-1210-52/ME:5#
```

create snmp host

Purpose	To create a recipient of SNMP traps generated by the Switch’s SNMP agent.
Syntax	**create snmp host <ipaddr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]**
Description	The **create snmp host** command creates a recipient of SNMP traps generated by the Switch’s SNMP agent.
Parameters	*<ipaddr>* − The IP address of the remote management station to serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − ensures that packets have not been tampered with during transit. • Authentication − determines if an SNMP message is from a valid source. • Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source. *<username 32>* − A string of up to 32 alphanumeric characters that identifies user name of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch’s SNMP agent. *noauth_nopriv* − Specifies that there is no authorization and no

	encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are encrypted.
Restrictions	Only Administrator, operator and powe user-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-1210-52/ME:5# create snmp host 10.90.90.90 v3 noauth_nopriv
dlink
Command: create snmp host 10.90.90.90 v3 noauth_nopriv dlink



Success.
DES-1210-52/ME:5#
```

delete snmp host

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

Example usage:

To delete an SNMP host:

```
DES-1210-52/ME:5# delete snmp host 10.90.90.90
Command: delete snmp host 10.90.90.90



Success.
DES-1210-52/ME:5#
```

show snmp host

Purpose	To display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp host {<ipaddr>}**
Description	The **show snmp host** command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps generated by the Switch's SNMP agent.

Parameters	*<ipaddr>* − The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DES-1210-52/ME:5# show snmp host
Command: show snmp host


SNMP Host Table
(Maximum Entries : 10)
Host IP Address    SNMP Version      Community Name/SNMPv3 User Name
---------------    ---------------   ---------------------------------------
10.90.90.90        V3-NoAuthNoPriv dlink


Total Entries : 1

DES-1210-52/ME:5#
```

create snmp v6host

Purpose	To create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**create snmp v6host <ip6_addr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]**
Description	The **create snmp v6host** command creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipv6_addr>* − The IPv6 address of the remote management station to serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − ensures that packets have not been tampered with during transit. • Authentication − determines if an SNMP message is from a valid source. • Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source. *<username 32>* − A string of up to 32 alphanumeric characters that

	identifies user name of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are encrypted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-1210-52/ME:5# create snmp v6host 3000::1 v3 noauth_nopriv dlink
Command: create snmp v6host 3000::1 v3 noauth_nopriv dlink



Success.
DES-1210-52/ME:5#
```

delete snmp v6host

Purpose	To remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**delete snmp v6host <ip6_addr>**
Description	The **delete snmp host** command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipv6_addr>* − The IPv6 address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an SNMP host entry:

```
DES-1210-52/ME:5# delete snmp v6host 3000::1
Command: delete snmp v6host 3000::1



Success.
DES-1210-52/ME:5#
```

show snmp v6host

Purpose	To display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp v6host {<ip6_addr>}**
Description	The **show snmp host** command is used to display the IPv6 addresses and configuration information of remote SNMP managers

	that are designated as recipients of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ip6_addr>* − The IPv6 address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DES-1210-52/ME:5# show snmp v6host
Command: show snmp v6host


SNMP Host Table
(Maximum Entries : 10)
Host IP Address              SNMP Version      Community or User Name
-----------------------------  ----------------  ------------------------------
3000::1                      V3-NoAuthNoPriv   dlink

Success.
DES-1210-52/ME:5#
```

enable trusted_host

Purpose	To enable the trusted host.
Syntax	**enable trusted_host**
Description	The **enable trusted_host** command enables the trusted host feature.
Parameters	None.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To enable the trusted host on the Swtich:

```
DES-1210-52/ME:5# enable trusted_host
Command: enable trusted_host


Success.
DES-1210-52/ME:5#
```

disable trusted_host

Purpose	To enable the trusted host.
Syntax	**disable trusted_host**
Description	The **disable trusted_host** command disables the trusted host feature.
Parameters	None.

Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To disable the trusted host on the Swtich:

```
DES-1210-52/ME:5# disable trusted_host
Command: disable trusted_host



Success.
DES-1210-52/ME:5#
```

create trusted_host

Purpose	To create a trusted host.
Syntax	**create trusted_host [<ipaddr> | network <network_address> | <ipv6_addr> | ipv6_prefix <ipv6networkaddr>]**
Description	The **create trusted_host** command creates a trusted host. The Switch allows specifying up to 30 IPv4 or IPv6 addresses that are allowed to manage the Switch via in-band 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 IPv4 address of the trusted host to be created. <*network_address*> − The subnet mask of the trusted host to be created. This parameter is optional. If not specified, the default subnet mask is 255.255.255.0. <*ipv6_addr*> − The IPv6 address of the trusted host to be created. *ipv6_prefix <ipv6networkaddr>* − The IPv6 subnet prefix of the trusted network to be created. The network address of the trusted network. The form of 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-1210-52/ME:5# create trusted_host 10.90.90.91
Command: create trusted_host 10.90.90.91

Success.
DES-1210-52/ME:5#
```

To create the IPv6 trusted host:

```
DES-1210-52/ME:5# create trusted_host 3000::1
Command: create trusted_host 3000::1



Success.
DES-1210-52/ME:5#
```

show trusted_host

Purpose	To display a list of trusted hosts entered on the Switch using the create trusted_host command above.
Syntax	**show trusted_host**
Description	The **show trusted_host** command displays 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-1210-52/ME:5# show trusted_host
Command: show trusted_host


Trusted Host Status : Disable

Management Stations

IP Address                 Subnet Mask
-----------------------------  -----------------------------
10.90.90.91                 255.255.255.255
3000::1                     128

Total Entries: 2

DES-1210-52/ME:5#
```

delete trusted_host

Purpose	To delete a trusted host entry made using the **create trusted_host** command above.
Syntax	**delete trusted_host [<ipaddr> | network <network_address> | <ipv6_addr> | ipv6_prefix <ipv6networkaddr> | all]**
Description	The **delete trusted_host** command deletes a trusted host entry made using the **create trusted_host** command above.
Parameters	*<ipaddr>* − The IP address of the trusted host. *all* − The all IP address of the trusted host. *network <network_address>* − The subnet mask of the trusted host to be deleted. This parameter is optional. *<ipv6_addr>* − The IPv6 address of the trusted host to be removed. *ipvv6_prefix <ipv6networkaddr>* − The IPv6 subnet prefix address of the trusted network to be removed. The network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To delete a trusted host with an IPv4 address **10.90.90.91**:

```
DES-1210-52/ME:5# delete trusted_host 10.90.90.91
Command: delete trusted_host 10.90.90.91

Success.
DES-1210-52/ME:5#
```

To delete a trusted host with an IPv6 address 3000::1:

```
DES-1210-52/ME:5# delete trusted_host 3000::1
Command: delete trusted_host 3000::1



Success.
DES-1210-52/ME:5#
```

enable snmp traps

Purpose	To enable SNMP trap support.
Syntax	**enable snmp traps**
Description	The **enable snmp traps** command enables 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-1210-52/ME:5# enable snmp traps
Command: enable snmp traps

Success.
DES-1210-52/ME:5#
```

disable snmp traps

Purpose	To disable SNMP trap support on the Switch.
Syntax	**disable snmp traps**
Description	The **disable snmp traps** command disables 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-1210-52/ME:5# disable snmp traps
Command: disable snmp traps

Success.
```

```
DES-1210-52/ME:5#
```

enable snmp authenticate_traps

Purpose	To enable SNMP authentication traps support.
Syntax	**enable snmp authenticate_traps**
Description	The **enable snmp authenticate_traps** command enables SNMP authentication trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To turn on SNMP authentication trap support:

```
DES-1210-52/ME:5# enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.
DES-1210-52/ME:5#
```

disable snmp authenticate_traps

Purpose	To disable SNMP authentication traps support.
Syntax	**disable snmp authenticate_traps**
Description	The **disable snmp authenticate_traps** command disables SNMP authentication trap 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-1210-52/ME:5# disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.
DES-1210-52/ME:5#
```

show snmp traps

Purpose	To display SNMP trap support status on the Switch.
Syntax	**show snmp traps**
Description	The **show snmp traps** command displays the SNMP trap support status currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DES-1210-52/ME:5# show snmp traps
Command: show snmp traps


SNMP Traps                                  : Enable
SNMP Authentication Traps                   : Enable
System Device Bootup                        : Enable
Fiber Port Link Up / Link Down              : Enable
Twisted Pair Port Link Up / Link Down       : Enable
RSTP Port State Change                      : Enable
Firmware Upgrade State                      : Enable
Port Security violation State               : Enable
IMPB violation State                        : Enable
Loopback detection State                    : Enable
DHCP server screening State                 : Enable
Duplicate IP Detected State                 : Enable

DES-1210-52/ME:5#
```

enable snmp linkchange_traps

Purpose	To enable SNMP link change traps support on the Switch.
Syntax	**enable snmp linkchange_traps**
Description	The **enable snmp linkchange_traps** command is used to enable SNMP link change traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the SNMP link change trap function:

```
DGS-1210-28P/ME:5# enable snmp linkchange_traps
Command: enable snmp linkchange_traps


Success.
DGS-1210-28P/ME:5#
```

disable snmp linkchange_traps

Purpose	To disable SNMP link change traps support on the Switch.
Syntax	**disable snmp linkchange_traps**
Description	The **disable snmp linkchange_traps** command is used to disable SNMP link change traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the SNMP link change trap function:

```
DGS-1210-28P/ME:5# disable snmp linkchange_traps
Command: disable snmp linkchange_traps



Success.
DGS-1210-28P/ME:5#
```

config snmp linkchange_traps ports

Purpose	To configure SNMP traps support on the Switch.
Syntax	**config snmp linkchange_traps ports [<portlist> | all] [enable | disable]**
Description	The **config snmp linkchange_traps ports** command configures the SNMP trap support status currently configured on the Switch.
Parameters	*[<portlist> | all]* – Specifies a port, ports or port range to be configured. *[enable | disable]* – Enable or disable the SNMP trap support for specified port.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the current SNMP trap settings:

```
DES-1210-52/ME:5# config snmp linkchange_traps ports 8-10 enable
Command: config snmp linkchange_traps ports 8-10 enable



Success.
DES-1210-52/ME:5#
```

show snmp traps linkchange_traps

Purpose	To show SNMP traps support on the Switch.
Syntax	**show snmp traps linkchange_traps**
Description	The **show snmp traps** command displays the SNMP trap support status currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DES-1210-52/ME:5# show snmp traps linkchange_traps
Command: show snmp traps linkchange_traps



Linkchange Traps   : Disable
  Port 01: Disabled
  Port 02: Disabled
  Port 03: Disabled
  Port 04: Disabled
  Port 05: Disabled
  Port 06: Disabled
  Port 07: Disabled
  Port 08: Enabled
  Port 09: Enabled
  Port 10: Enabled
  Port 11: Disabled
  Port 12: Disabled
  Port 13: Disabled
  Port 14: Disabled
  Port 15: Disabled
  Port 16: Disabled
  Port 17: Disabled
  Port 18: Disabled
  Port 19: Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

config snmp system_contact

Purpose	To enter the name of a contact person who is responsible for the Switch.
Syntax	**config snmp system_contact <string 128>**
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 128 character can be used.
Parameters	*<string 128>* − A maximum of 128 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**":

```
DES-1210-52/ME:5# config snmp system_contact MIS
Command: config snmp system_contact MIS


Success.
DES-1210-52/ME:5#
```

config snmp system_location

Purpose	To enter a description of the location of the Switch.
Syntax	**config snmp system_location <string 128>**
Description	The **config snmp system_ location** command is used to enter a description of the location of the Switch. A maximum of 20

	characters can be used.
Parameters	*<string 128>* − A maximum of 128 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch location to "**HQ**":

```
DES-1210-52/ME:5# config snmp system_location HQ
Command: config snmp system_location HQ


Success.
DES-1210-52/ME:5#
```

config snmp system_name

Purpose	To configure the name of the location of the Switch.
Syntax	**config snmp system_name <string 128>**
Description	The **config snmp system_ name** command configures the name of the Switch.
Parameters	*<string 128>* − A maximum of 128 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch name for "DES-1210:

```
DES-1210-52/ME:5# config snmp system_name DES-1210
Command: config snmp system_name DES-1210


Success.
DES-1210-52/ME:5#
```

config snmp warmstart_traps

Purpose	To enable or disable the warm start traps of SNMPon the Switch.
Syntax	**config snmp warmstart_traps [enable | disable]**
Description	The **config snmp warmstart_traps** command enable or disable the warm start traps of the Switch.
Parameters	*[enable | disable]* – Enable or disable the warm start traps of the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP warm start traps for the Switch:

```
DES-1210-52/ME:5# config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

```

```

Success.
DES-1210-52/ME:5#
```

config snmp coldstart_traps

Purpose	To enable or disable the cold start traps of SNMPon the Switch.
Syntax	**config snmp coldstart_traps [enable | disable]**
Description	The **config snmp coldstart_traps** command enable or disable the cold start traps of the Switch.
Parameters	*[enable | disable]* – Enable or disable the cold start traps of the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP cold start traps for the Switch:

```
DES-1210-52/ME:5# config snmp coldstart_traps disable
Command: config snmp coldstart_traps disable


Success.
DES-1210-52/ME:5#
```

enable snmp

Purpose	To enable SNMP support.
Syntax	**enable snmp**
Description	The **enable snmp** command enables SNMP support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP support on the Switch:

```
DES-1210-52/ME:5# enable snmp
Command: enable snmp

Success.
DES-1210-52/ME:5#
```

disable snmp

Purpose	To disable SNMP support.
Syntax	**disable snmp**
Description	The **disable snmp** command enables SNMP support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP support on the Switch:

```
DES-1210-52/ME:5# disable snmp
Command: disable snmp

Success.
DES-1210-52/ME:5#
```

enable snmp DHCP_ screening traps

Purpose	To enable SNMP DHCP screening traps.
Syntax	**enable snmp DHCP_screening traps**
Description	The **enable snmp DHCP_screening traps** command enables SNMP DHCP screening traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP DHCP screening traps support on the Switch:

```
DES-1210-52/ME:5# enable snmp DHCP_screening traps
Command: enable snmp DHCP_screening traps


Success.
DES-1210-52/ME:5#
```

disable snmp DHCP_ screening traps

Purpose	To disable SNMP DHCP screening traps.
Syntax	**disable snmp DHCP_screening traps**
Description	The **disable snmp DHCP_screening traps** command enables SNMP DHCP screening traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP DHCP screening traps support on the Switch:

```
DES-1210-52/ME:5# disable snmp DHCP_screening traps
Command: disable snmp DHCP_screening traps


Success.
DES-1210-52/ME:5#
```

enable snmp DHCPv6_ screening traps

Purpose	To enable SNMP DHCPv6 screening traps.

Syntax	**enable snmp DHCPv6_screening traps**
Description	The **enable snmp DHCPv6_screening traps** command enables SNMP DHCPv6 screening traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP DHCPv6 screening traps support on the Switch:

```
DES-1210-52/ME:5# enable snmp DHCPv6_screening traps
Command: enable snmp DHCPv6_screening traps



Success.
DES-1210-52/ME:5#
```

disable snmp DHCPv6_ screening traps

Purpose	To disable SNMP DHCPv6 screening traps.
Syntax	**disable snmp DHCPv6_screening traps**
Description	The **disable snmp DHCPv6_screening traps** command enables SNMP DHCPv6 screening traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP DHCPv6 screening traps support on the Switch:

```
DES-1210-52/ME:5# disable snmp DHCPv6_screening traps
Command: disable snmp DHCPv6_screening traps



Success.
DES-1210-52/ME:5#
```

enable snmp IMPB_violation traps

Purpose	To enable SNMP IMPB violation traps.
Syntax	**enable snmp IMPB_violation traps**
Description	The **enable snmp IMPBv2 traps** command enables SNMP IMPB violation traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP IMPB violation traps support on the Switch:

```
DES-1210-52/ME:5# enable snmp IMPB_violation traps
Command: enable snmp IMPB_violation traps
```

```

Success.
DES-1210-52/ME:5#
```

disable snmp IMPB_violation traps

Purpose	To disable SNMP IMPB violation traps.
Syntax	**disable snmp IMPB_violation traps**
Description	The **disable snmp IMPB_violation traps** command enables SNMP IMPB violation traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP IMPB violation traps support on the Switch:

```
DES-1210-52/ME:5# disable snmp IMPB_violation traps
Command: disable snmp IMPB_violation traps


Success.
DES-1210-52/ME:5#
```

enable snmp firmware_upgrade_state traps

Purpose	To enable SNMP firmware upgrade state traps.
Syntax	**enable snmp firmware_upgrade_state traps**
Description	The **enable snmp firmware_upgrade_state traps** command enables SNMP firmware upgrade state traps support on the Switch. After enables the SNMP firmware upgrade state traps support, the Switch will send out a trap to the SNMP manage host when the firmware upgrade is succeed or fail.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP firmware upgrade state traps support on the Switch:

```
DES-1210-52/ME:5# enable snmp firmware_upgrade_state traps
Command: enable snmp firmware_upgrade_state traps


Success.
DES-1210-52/ME:5#
```

disable snmp firmware_upgrade_state traps

Purpose	To disable SNMP firmware upgrade state traps.
Syntax	**disable snmp firmware_upgrade_state traps**

Description	The **disable snmp firmware_upgrade_state traps** command disables SNMP firmware upgrade state traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP firmware upgrade state traps support on the Switch:

```
DES-1210-52/ME:5# disable snmp firmware_upgrade_state traps
Command disable enable snmp firmware_upgrade_state traps



Success.
DES-1210-52/ME:5#
```

enable snmp LBD traps

Purpose	To enable SNMP LBD traps.
Syntax	**enable snmp LBD traps**
Description	The **enable snmp LBD traps** command enables SNMP LBD traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP LBD traps support on the Switch:

```
DES-1210-52/ME:5# enable snmp LBD traps
Command: enable snmp LBD traps



Success.
DES-1210-52/ME:5#
```

disable snmp LBD traps

Purpose	To disable SNMP LBD traps.
Syntax	**disable snmp LBD traps**
Description	The **disable snmp LBD traps** command disables SNMP LBD traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP LBD traps support on the Switch:

```
DES-1210-52/ME:5# disable snmp LBD traps
Command: disable snmp LBD traps
```

```
Success.
DES-1210-52/ME:5#
```

enable snmp port_security_violation traps

Purpose	To enable SNMP port security violation traps.
Syntax	**enable snmp port_security_violation traps**
Description	The **enable snmp port_security_violation traps** command enables SNMP port security violation traps on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP port security violation traps support on the Switch:

```
DES-1210-52/ME:5# enable snmp port_security_violation traps
Command: enable snmp port_security_violation traps



Success.
DES-1210-52/ME:5#
```

disable snmp port_security_violation traps

Purpose	To disable SNMP port security violation traps.
Syntax	**disable snmp port_security_violation traps**
Description	The **disable snmp port_security_violation traps** command disables SNMP port security violation traps on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP port security violation traps support on the Switch:

```
DES-1210-52/ME:5# disable snmp port_security_violation traps
Command: disable snmp port_security_violation traps



Success.
DES-1210-52/ME:5#
```

enable snmp rstpport_state_change traps

Purpose	To enable SNMP rstp port state change traps support on the Switch.
Syntax	**enable snmp rstpport_state_change traps**
Description	The **enable snmp rstpport_state_change traps** command enables SNMP rstp port state change traps support on the Switch. After enables the SNMP RSTP port state change traps support, the Switch will send out a trap when the state of RSTP port is changed.

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

Example usage:

To enable SNMP RSTP port state change traps support on the Switch:

```
DES-1210-52/ME:5# enable snmp rstpport_state_change traps
Command: enable snmp rstpport_state_change traps



Success.
DES-1210-52/ME:5#
```

disable snmp rstpport_state_change traps

Purpose	To disable SNMP RSTP port state change traps.
Syntax	**disable snmp rstpport_state_change traps**
Description	The **disable snmp rstpport_state_change traps** command disables SNMP RSTP port state change traps on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP RSTP port state change traps support on the Switch:

```
DES-1210-52/ME:5# disable snmp rstpport_state_change traps
Command: disable snmp rstpport_state_change traps



Success.
DES-1210-52/ME:5#
```

enable snmp duplicate_IP_detected traps

Purpose	To enable SNMP duplicate IP detected traps support on the Switch.
Syntax	**enable snmp duplicate_IP_detected traps**
Description	The **enable snmp duplicate_IP_detected traps** command enables SNMP duplicate IP detected traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the SNMP duplicate_IP_detected traps on the Switch:

```
DES-1210-52/ME:5# enable snmp duplicate_IP_detected traps
Command: enable snmp duplicate_IP_detected traps



Success.
DES-1210-52/ME:5#
```

disable snmp duplicate_IP_detected traps

Purpose	To disable SNMP duplicate IP detected traps support on the Switch.
Syntax	**disable snmp duplicate_IP_detected traps**
Description	The **disable snmp duplicate_IP_detected traps** command disables SNMP duplicate IP detected traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the SNMP duplicate_IP_detected traps on the Switch:

```
DES-1210-52/ME:5# disable snmp duplicate_IP_detected traps
Command: disable snmp duplicate_IP_detected traps



Success.
DES-1210-52/ME:5#
```

15

DOWNLOAD/UPLOAD COMMANDS

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

Command	Parameter
download	[cfg_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64> config_id <value 1-2>] | [firmware_ fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64> image_id <value 1-2>]
upload	[[firmware_toTFTP [<ipaddr> | <ip6_addr>] <path_filename 64> image_id <value 1-2>] | [cfg_toTFTP [<ipaddr> | <ip6_addr>] <path_filename 64> config_id <value 1-2>] | [log_toTFTP [<ipaddr> | <ip6_addr>] <path_filename 64>]]
config configuration config_id	<value 1-2> [boot_up | delete]
show firmware information	
show config	[current_config | config_in_nvram config_id <value 1-2> {[begin | exclude | include] <string 80>}
show boot_file	
config firmware image_id	<value 1-2> [boot_up | delete]

Each command is listed in detail, as follows:

download	
Purpose	To download and install a firmware, boot, or switch configuration file from a TFTP server.
Syntax	**download [cfg_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64> config_id <value 1-2>] | [firmware_ fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64> image_id <value 1-2>]**
Description	The **download** command downloads a firmware, boot, or switch configuration file from a TFTP server.
Parameters	*cfg_fromTFTP* − Downloads a switch configuration file from a TFTP server. *<ipaddr>* − The IPv4 address of the TFTP server. *<ipv6_addr>* − The IPv6 address of the TFTP server. *<path_filename 64>* − The DOS path and filename of the switch configuration file, up to 64 characters, on the TFTP server. For example, C:\ DES-1210-52ME-C1-20-01-B052-ALL.hex. *config_id <value 1-2>* − Specify the config id to be download. *firmware_fromTFTP* − Downloads and installs firmware on the Switch from a TFTP server. *< path_filename 64>* − The DOS path and filename of the firmware

	file, up to 64 characters, on the TFTP server. For example, C:\ DES-1210-52ME-C1-20-01-B052-ALL.hex. *image_id <value 1-2>* − Specify the image id to be download.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To download a firmware file:

```
DES-1210-52/ME:5# download firmware_fromTFTP 172.21.45.73 DES-1210-52ME-C1-20-01-B054-ALL.hex image_id 1
Command: download firmware_fromTFTP 172.21.45.73 DES-1210-52ME-C1-20-01-B054-ALL.hex image_id 1

Connecting to server…………………..Done.
Download firmware…………………..…..Done.  Do not power off!
Please wait, programming flash……Done.

Success.
Image Updated Successful

DES-1210-52/ME:5#
```

To download a configuration file:

```
DES-1210-52/ME:5# download configuration 10.48.74.121 c:\cfg\setting.txt
Overwrite file [startup-config] ?[Yes/press any key for no]....
01-Jan-200003:19:46%COPY-I-FILECPY:FilesCopy-source URL tftp://10.48.74.121/1.txt destination
URL flash://startup-config
Success.

Success.

.....01-Jan-2000 03:18:40 %COPY-N-TRAP: The copy operation was completed Success.fully!
Copy: 267 bytes copied in 00:00:08 [hh:mm:ss]
DES-1210-52/ME:5#
```

upload	
Purpose	To upload the current switch settings to a TFTP server.
Syntax	**upload [[firmware_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64> image_id <value 1-2>] | [cfg_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64> config_id <value 1-2>] | [log_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>]]**
Description	The **upload** command uploads the Switch's current settings to a TFTP server.
Parameters	*firmware_toTFTP* − Specifies that the Switch's current firmware are to be uploaded to the TFTP server. *<ipaddr>* − The IPv4 address of the TFTP server. The TFTP server

	must be on the same IP subnet as the Switch. *<ipv6_addr>* − The IPv6 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. *<path_filename 64>* − The location of the Switch configuration file on the TFTP server. *image_id <value 1-2>* - Specifies the image id which to be uploaded. *config_id <value 1-2>* − Specifies the config id which to be uploaded.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

```
DES-1210-52/ME:5# upload log_toTFTP 172.21.45.73 log1
Command: upload log_toTFTP 172.21.45.73 log1

Success.
DES-1210-52/ME:5#
```

config configuration config_id

Purpose	Used to delete the specific firmware or configure the specific firmware as boot up image.
Syntax	**config configuration config_id <value 1-2> [boot_up | delete]**
Description	The **config configuration config_id** command is used to delete the specific firmware or configure the specific firmware as boot up image.
Parameters	*<value 1-2>* − Specifies the serial number of the indicated configuration. *[boot_up* | *delete]* − Specifies the config is boot_up config or delete the specified configuration.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

```
DES-1210-52/ME:5# config configuration config_id 1 boot_up
Command: config configuration config_id 1 boot_up


Success.
DES-1210-52/ME:5#
```

show firmware information

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

Example usage:

```
DES-1210-52/ME:5# show firmware information
Command: show firmware information

Current          : image one
Configured       : image one

IMAGE ONE        :
Version          : 20.01.B054
Size             : 8640608 Bytes
Updated Time : 01/01/2014 00:04:48
From             : 10.90.90.98
User             : Anonymous (web)

IMAGE TWO        :
Version          : 20.01.B054
Size             : 8271800 Bytes
Updated Time : 01/01/2014 00:05:50
From             : 10.90.90.99
User             : Anonymous (web)

DES-1210-52/ME:5#
```

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 <value 1-2> {[begin | exclude | include] <string 80>}**
Description	The **show config** command is used 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).
Parameters	None.
Restrictions	Only Administrator -level users can issue this command.

Example usage:

```
DES-1210-52/ME:5# show config current_config
Command: show config current_config




#-------------------------------------------------------------------------------------------------
#              DES-1210-52/ME Fast Ethernet Switch Configuration
#
#                        Firmware: Build 20.01.B054
#        Copyright(C) 2010 D-Link Corporation. All rights reserved.
#-------------------------------------------------------------------------------------------------
```

```
command-start

# User Account
disable password encryption



# Basic
config syslogintimeout 5
config sysgroupinterval 0
enable web 80
enable clipaging
config command_prompt default
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

show boot_file

Purpose	Used to display the configuration file and firmware image assigned as boot up files.
Syntax	**show boot_file**
Description	The **show boot_file** command is used to display the configuration file and firmware image assigned as boot up files.
Parameters	None.
Restrictions	None.

Example usage:

To display the configuration file and firmware image assigned as a boot up file:

```
DGS-1210-28P/ME:5# show boot_file
Command: show boot_file

Bootup Firmware : image_1
Bootup Configuration : config_1
DGS-1210-28P/ME:5#
```

config firmware image_id

Purpose	Used to configure the firmware image id.
Syntax	**config firmware image_id <value 1-2> [boot_up | delete]**
Description	The **config firmware image_id** command is used to configure the firmware image id
Parameters	<*value 1-2*> - Specify the image id to be configured. *[boot_up* | *delete]* – Specify to boot up or delete the specified image id.
Restrictions	Only Administrator -level users can issue this command.

Example usage:

```
DES-1210-52/ME:5# config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up
```

```
Success.
DES-1210-52/ME:5#
```

16

DHCP RELAY COMMANDS

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

Command	Parameter
enable dhcp_relay	
disable dhcp_relay	
config dhcp_relay port	<portlist> state [enable | disable]
config dhcp_relay add ipif System	<ipaddr>
config dhcp_relay delete ipif System	<ipaddr>
config dhcp_relay hops	<value 1-16>
config dhcp_relay vlan	[<vlan_name 32> | vlanid <vidlist>] state [enable | disable]
config dhcp_relay option_82	[check [enable | disable] | policy [drop | keep | replace] | remote_id [default | user_define <desc 32>] | state [enable | disable] | circuit_id [default | user_define <desc 32>]]
config dhcp_relay port_option_82	{<portlist>} [circuit_id | remote_id] vendor3 <desc 32>
show dhcp_relay port_option_82	{<portlist>}
show dhcp_relay	{ipif}
enable dhcp_local_relay	
disable dhcp_local_relay	
config dhcp_local_relay port	port <portlist> state [enable | disable]
config dhcp_local_relay vlan	[<vlan_name 32> | vlanid <vidlist>] state [enable | disable]
show dhcp_local_relay	
enable dhcpv6_relay	
disable dhcpv6_relay	
show dhcpv6_relay	{ipif System | option_38 ports <portlist>}
config dhcpv6_relay	[add | delete] ipif system <ip6_addr>
config dhcpv6_relay hop_count	<value 1-32>
config dhcpv6_relay option_37	[check | state] [enable | disable] | remote_id [default | user_define <string 128> | cid_with_user_define <string 128>]]

Command	Parameter
config dhcpv6_relay option_38	ports <portlist> [state [enable | disable] | subscriber_id [default | user_define]]
show dhcpv6_relay option_38	{ports <portlist>}

Each command is listed in detail, as follows:

enable dhcp_relay

Purpose	To enable DHCP Relay server on the Switch
Syntax	**enable dhcp_relay**
Description	The **enable dhcp_relay** command sets the DHCP Relay to be globally enabled on the Switch and on all existing VLANs.
Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To enable DCHP Relay on the Switch:

```
DES-1210-52/ME:5# enable dhcp_relay
Command: enable dhcp_relay



Success.
DES-1210-52/ME:5#
```

disable dhcp_relay

Purpose	To disable DHCP Relay server on the Switch
Syntax	**disable dhcp_relay**
Description	The **disable dhcp_relay** command sets the DHCP Relay to be globally disabled on the Switch and on all existing VLANs.
Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To disable DHCP Relay on the Switch:

```
DES-1210-52/ME:5# disable dhcp_relay
Command: disable dhcp_relay



Success.
DES-1210-52/ME:5#
```

config dhcp_relay port

Purpose	**To enable or disable the ports of DHCP Relay server.**
Syntax	**config dhcp_relay port <portlist> state [enable | disable]**
Description	The **config dhcp_relay** port command is used to enable or disable the ports of DHCP Relay server.
Parameters	*<portlist>* − Specifies the ports to be configured. *state [enable* | *disable]* – Specifies the ports of DHCP Relay server to be enabled or disabled.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To enable ports 1-4 of DHCP Relay server:

```
DES-1210-52/ME:5# config dhcp_relay port 1-4 state enable
Command: config dhcp_relay port 1-4 state enable



Success.

DES-1210-52/ME:5#
```

config dhcp_relay add ipif System

Purpose	**To define a DHCP server as a DHCP Relay server**
Syntax	**config dhcp_relay add ipif System <ipaddr>**
Description	The **config dhcp_relay add ipif System** command adds DHCP servers as DHCP Relay servers.
Parameters	*<ipaddr>* − The IP address of the DHCP server. Up to 4 servers can be defined.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To add a DHCP server as a DHCP Relay server:

```
DES-1210-52/ME:5# config dhcp_relay add ipif System 10.90.90.95
Command: config dhcp_relay add ipif System 10.90.90.95



Success.

DES-1210-52/ME:5#
```

config dhcp_relay delete ipif System

Purpose	To delete a DHCP server from the DHCP Relay server list.
Syntax	**config dhcp_relay delete ipif System <ipaddr>**
Description	The **config dhcp_relay delete ipif System** command deletes a DHCP servers defined as a DHCP Relay server.
Parameters	*<ipaddr>* − The IP address of the DHCP server.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To remove a DHCP server from the DHCP Relay server list:

```
DES-1210-52/ME:5# config dhcp_relay delete ipif System 10.6.150.49
Command: config dhcp_relay delete ipif System 10.6.150.49



Success.
DES-1210-52/ME:5#
```

config dhcp_relay hops

Purpose	To delete a DHCP server from the DHCP Relay server list.
Syntax	**config dhcp_relay hops <value 1-16>**
Description	The **config dhcp_relay hops** command configures the DHCP/BOOTP relay feature.
Parameters	*hops <value 1-16>* − Specifies the maximum number of relay agent hops that the DHCP packets can cross.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure the DHCP relay hops on the Switch:

```
DES-1210-52/ME:5# config dhcp_relay hops 12
Command: config dhcp_relay hops 12

Success.
DES-1210-52/ME:5#
```

config dhcp_relay vlan

Purpose	To configure a VLAN of DHCP Relay to be enabled or disabled of the Switch.
Syntax	**config dhcp_relay vlan [<vlan_name 32> | vlanid <vidlist>] state [enable | disable]**
Description	The **config dhcp_relay vlan** command configures a VLAN of DHCP Relay to be enabled or disable of the Switch.
Parameters	*<vlan_name 32>* − Specifies the VLAN name to be configured.

	vlanid <vidlist> - Specifies the id of VLAN to be configured. *[enable | disable]* – Specifies the VLAN of DHCP Relay to be enabled or disabled.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To specify the VLAN ID 2 of DHCP relay to be enabled:

```
DES-1210-52/ME:5# config dhcp_relay vlan vlanid 2 state enable
Command: config dhcp_relay vlan vlanid 2 state enable



Success.

DES-1210-52/ME:5#
```

config dhcp_relay option_82

Purpose	To configure the check, policy and state of DHCP relay agent information option 82 of the Switch.
Syntax	**config dhcp_relay option_82 [check [enable | disable] | policy [drop | keep | replace] | remote_id [default | user_define <desc 32>] | state [enable | disable] | circuit_id [default | user_define <desc 32>]]**
Description	The **config dhcp_relay option_82** is used to configure the check, policy and state of DHCP relay agent information option 82 of the Switch
Parameters	*check:* used to configure the check of DHCP relay agent information option 82 of the Switch. *enable* – When the field is toggled to enable, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option 82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *disable* – When the field is toggled to disable, the relay agent will not check the validity of the packet's option 82 field. policy: used to configure the re-forwarding policy of DHCP relay agent information option 82 of the Switch. *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. state: used to configure the state of DHCP relay agent information option 82 of the Switch. *enable* − When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in

	messages between DHCP server and client. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *disable* − If the field is toggled to disable the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect. *circuit_id [default* | *user_define <desc 32>]* **-**
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To disable the DHCP relay option 82 on the Switch:

```
DES-1210-52/ME:5# config dhcp_relay option_82 state disable
Command: config dhcp_relay option_82 state disable



Success.

DES-1210-52/ME:5#
```

config dhcp_relay port_option_82

Purpose	To configure DHCP relay agent option 82 information of each port.
Syntax	**config dhcp_relay port_option_82 {<portlist>} [circuit_id | remote_id] vendor3 <desc 32>**
Description	The **config dhcp_relay port_option_82** is used to configure DHCP relay agent option 82 information of each port.
Parameters	*<portlist>* – Specifies the ports' option 82 information. *circuit_id* – Specifies the content in the Circuit ID. *remote_id* – Specifies the content in the Remote ID. *vendor3 <desc 32>* – To configure a apecific ports' vendor3 user define string.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure vendor3 circuit_id of port 1 to "12345678":

```
DES-1210-28/ME:5# config dhcp_relay port_option_82 1 circuit_id
vendor3 12345678
```

```
Command: config dhcp_relay port_option_82 1 circuit_id vendor3
12345678



Success.

DES-1210-28/ME:5#
```

show dhcp_relay port_option_82

Purpose	To display the current DHCP Relay option 82 information of each port.
Syntax	**show dhcp_relay port_option_82 {<portlist>}**
Description	The **show dhcp_relay port_option_82** command displays the current DHCP Relay option 82 information of each port.
Parameters	<*portlist*> – Specifies the ports' option 82 information to be displayed.
Restrictions	None.

Example usage:

To display DHCP Relay option 82 information of port 1-3:

```
DES-1210-28/ME:5# show dhcp_relay port_option_82 1-3
Command: show dhcp_relay port_option_82 1-3


Port option 82 information of vendor 3

Port   Circuit ID                    Remote ID
----   ------------------------------ ------------------------------
1      12345678
2
3


DES-1210-28/ME:5#
```

show dhcp_relay

Purpose	To display the DHCP Relay settings on the Switch.
Syntax	**show dhcp_relay {ipif}**
Description	The **show dhcp_relay** command displays the DHCP Relay status and list of servers defined as DHCP Relay servers on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display DHCP Relay settings:

```
DES-1210-52/ME:5# show dhcp_relay
```

```
Command: show dhcp_relay


DHCP/BOOTP Relay Status              : Enabled
DHCP/BOOTP Relay Enable Portlist  : 1-52
DHCP/BOOTP Relay Enable VID List : 1,
DHCP/BOOTP Hops Count Limit       : 12
DHCP/BOOTP Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State    : Enabled
DHCP Relay Agent Information Option 82 Check    : Disabled
DHCP Relay Agent Information Option 82 Policy   : Replace
DHCP Relay Agent Information Option 82 ID
DHCP Relay Agent Information Option 82 Circuit ID Type   : Default
DHCP Relay Agent Information Option 82 Remote  ID Type   : Default

Interface    Server 1        Server 2        Server 3        Server 4
---------    ---------------  ---------------  ---------------  ---------------
System       10.90.90.95

DES-1210-52/ME:5#
```

enable dhcp_local_relay

Purpose	To enable the DHCP local relay feature globally.
Syntax	**enable dhcp_local_relay**
Description	The **enable dhcp_local_relay** command enables the DHCP local relay feature on the Switch.
Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To enable the DHCP Local Relay:

```
DES-1210-52/ME:5# enable dhcp_local_relay
Command: enable dhcp_local_relay


Success.
DES-1210-52/ME:5#
```

disable dhcp_local_relay

Purpose	To disable the DHCP local relay feature globally
Syntax	**disable dhcp_local_relay**
Description	The **disable dhcp_local_relay** command disables the DHCP local relay feature on the Switch.

Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To disable the DHCP Local Relay:

```
DES-1210-52/ME:5# disable dhcp_local_relay
Command: disable dhcp_local_relay


Success.
DES-1210-52/ME:5#
```

config dhcp_local_relay port

Purpose	To enable or disable the ports of DHCP Local Relay.
Syntax	**config dhcp_local_relay port <portlist> state [enable | disable]**
Description	The **config dhcp_local_relay port** command is used to enable or disable the ports of DHCP Local Relay.
Parameters	*<portlist>* – Specifies the ports to be enabled or disabled. *state [enable* | *disable]* – Enable or disable the specified ports of the DHCP Local Relay status.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To enable the port 8-10 of DHCP Local Relay:

```
DES-1210-52/ME:5# config dhcp_local_relay port 8-10 state enable
Command: config dhcp_local_relay port 8-10 state enable



Success.
DES-1210-52/ME:5#
```

config dhcp_local_relay vlan

Purpose	To specify which VLAN's the feature works on.
Syntax	**config dhcp_local_relay vlan [<vlan_name 32> | vlanid <vidlist>] state [enable | disable]**
Description	Each VLAN which was added to the DHCP Local Relay list participates in the DHCP Local Relay process – Option 82 is added to DHCP requests on this VLAN, and Removed from DHCP Replies on this VLAN.
Parameters	*[<vlan_name 32>* | *vlanid <vidlist>]* – Specify the vlan name or vlan id to be configured. *state [enable* | *disable]* – enable or disable of the DHCP Local Relay

	status by VLAN name or VLAN ID.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To disable the VLAN id 1 from VLAN of DHCP Local Relay:

```
DES-1210-52/ME:5# config dhcp_local_relay vlan vlanid 1 state disable
Command: config dhcp_local_relay vlan vlanid 1 state disable




Success.
DES-1210-52/ME:5#
```

show dhcp_local_relay

Purpose	To display which VLAN’s the feature works on.
Syntax	**show dhcp_local_relay**
Description	Each VLAN which was added to the DHCP Local Relay list participates in the DHCP Local Relay process – Option 82 is added to DHCP requests on this VLAN, and Removed from DHCP Replies on this VLAN.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP local relay information on the Switch:

```
DES-1210-52/ME:5# show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status   : Enabled
DHCP/BOOTP Local Relay PortList : None
DHCP/BOOTP Local Relay VID List :

DES-1210-52/ME:5#
```

enable dhcpv6_relay

Purpose	To enable DHCPv6 Relay function on the Switch
Syntax	**enable dhcpv6_relay**
Description	The **enable dhcpv6_relay** command is used to enable the DHCPv6 relay global state on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable DCHPv6 Relay on the Switch:

```
DES-1210-52/ME:5# enable dhcpc6_relay
Command: enable dhcpc6_relay


Success.

DES-1210-52/ME:5#
```

disable dhcpv6_relay

Purpose	To disable DHCPv6 Relay function on the Switch
Syntax	**disable dhcpv6_relay**
Description	The **disable dhcpv6_relay** command is used to disable the DHCPv6 relay global state on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable DHCPv6 Relay on the Switch:

```
DES-1210-52/ME:5# disable dhcpv6_relay
Command: disable dhcpv6_relay


Success.

DES-1210-52/ME:5#
```

show dhcpv6_relay

Purpose	To display the current DHCPv6 relay configuration.
Syntax	**show dhcpv6_relay {ipif system}**
Description	The **show dhcpv6_relay** command displays the current DHCPv6 relay configuration of all interfaces, or if an IP interface name is specified, the DHCPv6 relay configuration for that IP interface.
Parameters	None.
Purpose	To display the current DHCPv6 relay configuration.

Example usage:

To display DHCPv6 Relay settings:

```
DES-1210-52/ME:5# show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Relay Global State                : enable
DHCPv6 Hops Count Limit                  : 4
DHCPv6 Relay Option37 State              : enable
DHCPv6 Relay Option37 Check State        : enable
```

```
DHCPv6 Relay Option37 Remote ID Type : default
DHCPv6 Relay Option37 Remote ID         : 00-01-02-03-04-05
--------------------------------------------------------------
IP Interface            : Syetem
Server Address        :

 Total Entries   : 0

DES-1210-52/ME:5#
```

config dhcpv6_relay

Purpose	Used to add or delete a destination IP address to or from the switch's DHCPv6 relay table.
Syntax	**config dhcpv6_relay [add | delete] ipif System <ipv6_addr>**
Description	The **config dhcpv6_relay** command can add or delete an IPv6 destination address to forward (relay) DHCPv6 packets.
Parameters	*add* − Add an IPv6 destination to the DHCPv6 relay table. *delete* − Remove an IPv6 destination to the DHCPv6 relay table. *ipif System* − The name of the IP interface in which DHCPv6 relay is to be enabled. <*ipv6_addr*> − The DHCPv6 server IP address.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add the DHCPv6 relay on the Switch:

```
DES-1210-52/ME:5# config dhcpv6_relay add ipif System 3000::1
Command: config dhcpv6_relay add ipif System 3000::1



Success.

DES-1210-52/ME:5#
```

config dhcpv6_relay hop_count

Purpose	Used to configure the DHCPv6 relay hop count of the switch.
Syntax	**config dhcpv6_relay hop_count <value 1-32>**
Description	The **config dhcpv6_relay hops_count** command is used to configure the DHCPv6 relay hop count of the switch.
Parameters	<*value 1-32*> − The hop count is the number of relay agents that have to be relayed in this message. The range is 1 to 32. The default value is 4.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCPv6 relay hop count on the Switch:

```
DES-1210-52/ME:5# config dhcpv6_relay hop_count 3
```

```
Command: config dhcpv6_relay hop_count 3


Success.

DES-1210-52/ME:5#
```

config dhcpv6_relay option_18

Purpose	Used to configure the processing of Option 18 for the DHCPv6 relay function. Both the DHCPv6 relay and DHCPv6 local relay functions use the same Interface ID format. Localrelay isn't concerned about the option state it adds to the packet.
Syntax	**config dhcpv6_relay option_18 [check [enable | disable] | state [enable | disable] | interface_id [default | cid | vendor1]]**
Description	The **config dhcpv6_relay option_18** command is used to configure the processing of Option 18 for the DHCPv6 relay function. Both the DHCPv6 relay and DHCPv6 local relay functions use the same Interface ID format.
Parameters	*check [enable* | *disable]* – Specifies whether or not to check for the Option 18 field in incoming packets. *state [enable* | *disable]* – Specifies the DHCPv6 Relay Option 18's state. When the state is enabled, the DHCP packet will be inserted with the Option 18 field before being relayed to server. *interface_id* – Specify the format of the Interface ID. *default* - Specify to used the default formation for the Interface ID. *cid* - Specify to use the CID format for the Interface ID. *vendor1* - Specify to use the Vendor 1 format for the Interface ID.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCPv6 relay option 18 to be enabled on the Switch:

```
DES-1210-52/ME:5# config dhcpv6_relay option_18 state enable
Command: config dhcpv6_relay option_18 state enable


Success.

DES-1210-52/ME:5#
```

config dhcpv6_relay option_37

Purpose	Used to configure the DHCPv6 relay option_37 of the switch.
Syntax	**config dhcpv6_relay option_37 [check | state] [enable | disable] | remote_id [default | user_define <string 128> | cid_with_user_define <string 128>]]**
Description	The **config dhcpv6_relay hops_count** command is used to configure the DHCPv6 Relay option 37 function.When DHCPv6 relay option 37 is enabled, the DHCP packet is inserted with the option 37 field before being relayed to the server. The DHCP packet will be processed based on the behavior defined in the check and remote ID type setting. When the state is disabled, the DHCP packet is relayed directly to the server.
Parameters	*state [enable* | *disable]* - Specify DHCPv6 relay option37 state. When the state is enabled, the DHCP packet is inserted with the option 37 field before being relayed to the server. When the state is disabled, the DHCP packet is relayed directly to the server. *check [enable* | *disable]* - Specify to check the packets or not. When the check state is enabled, packets from client side should not have the option 37 field. If client originating packets have the option 37 field, they will be dropped. Specify for not checking the packets. *remote_id [default* | *cid_with_user_define <string 128>* | *user_define <string 128>]* - Specify the content in the remote ID. default – Specify to have the remote ID as VLAN ID + Module + Port +System MAC address of the device. cid_with_user_define – Specify to have the remote ID as VLAN ID + Module + Port + user defined string. user_define – Use the user-defined string as the remote ID.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCPv6 relay option_37 to be disabled on the Switch:

```
DES-1210-52/ME:5# config dhcpv6_relay option_37 state disable
Command: config dhcpv6_relay option_37 state disable



Success.

DES-1210-52/ME:5#
```

config dhcpv6_relay option_38

Purpose	Used to configure the DHCPv6 relay option_38 of the switch.
Syntax	**config dhcpv6_relay option_38 ports <portlist> [state [enable | disable] | subscriber_id [default | user_define]]**
Description	The **config dhcpv6_relay option_38** command is used to configure the DHCPv6 relay option_38 of the switch.
Parameters	*<portlist>* - Specify the ports to be configured. *state [enable* | *disable]* - Specify DHCPv6 relay option38 state. When the state is enabled, the DHCP packet is inserted with the

	option 38 field before being relayed to the server. When the state is disabled, the DHCP packet is relayed directly to the server. *subscriber_id [defult* | *user_define]* - Use the user-defined string as the subscriber ID.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCPv6 relay option_38 of ports 6~9 to be enabled on the Switch:

```
DES-1210-52/ME:5# config dhcpv6_relay option_38 ports 6-9 state enable
Command: config dhcpv6_relay option_38 ports 6-9 state enable



Success.

DES-1210-52/ME:5#
```

show dhcpv6_relay option_38

Purpose	Used to display the DHCPv6 relay option 38 of the switch.
Syntax	**show dhcpv6_relay option_38 {ports <portlist>}**
Description	The **show dhcpv6_relay option_38** command is used to display the DHCPv6 relay option 38 of the switch.
Parameters	*ports <portlist>* - Specifies the ports to be displayed.
Restrictions	None.

Example usage:

To display the DHCPv6 relay option 38 of ports 5-8 on the Switch:

```
DES-1210-52/ME:5# show dhcpv6_relay option_38 ports 5-8
Command: show dhcpv6_relay option_38 ports 5-8



DHCPv6 Relay Option38 Information

Port State    Type       Subscriber ID
-----  ---------  -------------- ----------------------
5    Disabled Default
6    Disabled Default
7    Disabled Default
8    Disabled Default



DES-1210-52/ME:5#
```

17

CPU PROTECTION COMMANDS

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

Command	Parameter
enable cpu_protect	
disable cpu_protect	
config cpu_protect	[arp | bpdu | icmp | igmp | snmp] pps [<value> | no_limit]
show cpu_protect	

Each command is listed in detail, as follows:

enable cpu_protect	
Purpose	To enable the CPU protection function on the Switch.
Syntax	**enable cpu_protect**
Description	The **enable cpu_protect** command is used to enable the CPU protection function on the Switch.
Parameters	None*.*
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To enable the CPU protection function on the switch:

```
DES-1210-52/ME:5# enable cpu_protect
Command: enable cpu_protect

Success.

DES-1210-52/ME:5#
```

disable cpu_protect	
Purpose	To disable the CPU protection function on the Switch.
Syntax	**disable cpu_protect**
Description	The **disable cpu_protect** command is used to disable the CPU protection function on the Switch.
Parameters	None*.*
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To disable the CPU protection function on the switch:

```
DES-1210-52/ME:5# disable cpu_protect
Command: disable cpu_protect

Success.

DES-1210-52/ME:5#
```

config cpu_protect type

Purpose	To configure the CPU protection packet type on the Switch.
Syntax	**config cpu_protect type [arp | bpdu | icmp | igmp | snmp] pps [<value> | no_limit]**
Description	The **config cpu_protect type** command is used to configure the CPU protection packet type on the Switch.
Parameters	*[arp* | *bpdu* | *icmp* | *snmp]* – Specifies the packet type of CPU protection to be configured*.* *[<value>* | *no_limit]* – Specifies the maximum packet number can be up to CPU.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the CPU protection with ARP type on the switch:

```
DES-1210-52/ME:5# config cpu_protect type arp pps no_limit
Command: config cpu_protect type arp pps no_limit

Success.

DES-1210-52/ME:5#
```

show cpu_protect

Purpose	To display the CPU protection information on the Switch.
Syntax	**show cpu_protect**
Description	The **show cpu_protect** command is used to display the CPU protection information on the Switch.
Parameters	None*.*
Restrictions	None.

Example usage:

To display the CPU protection information on the switch:

```
DES-1210-52/ME:5# show cpu_protect
Command: show cpu_protect

CPU Protect State   : Enabled

CPU Protect Type  Rate Limit(pps)
------------------------ ------------------------
ARP                      no limit
BPDU                     no limit
ICMP                     no limit
IGMP                     no limit
SNMP                     no limit


DES-1210-52/ME:5#
```

18

GRATUITOUS ARP COMMANDS

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

Command	Parameter
config gratuitous_arp send ipif_status_up	[enable | disable]
config gratuitous_arp send dup_ip_detected	[enable | disable]
config gratuitous_arp learning	[enable | disable]
enable gratuitous_arp	[log | trap]
disable gratuitous_arp	[log | trap]
show gratuitous_arp	
config gratuitous_arp send periodically	ipif <ipif_name 12> interval <integer 0-65535>

Each command is listed in detail, as follows:

config gratuitous_arp send ipif_status_up	
Purpose	Used to enable or disable the sending of gratuitous ARP requests while the IP interface status is up.
Syntax	**config gratuitous_arp send ipif_status_up [enable | disable]**
Description	The **config gratuitous_arp send ipif_status_up** command is used to enable or disable the sending of gratuitous ARP request packets while the IPIF interface is up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is enabled, and only one gratuitous ARP packet will be broadcast.
Parameters	*enable* − Enable the sending of gratuitous ARP when the IPIF status is up. *disable* − Disable the sending of gratuitous ARP when the IPIF status is up.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable a gratuitous ARP request:

```
DES-1210-52/ME:5# config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable


Success!
```

```
DES-1210-52/ME:5#
```

config gratuitous_arp send dup_ip_detected

Purpose	Used to enable or disable the sending of gratuitous ARP requests while duplicate IP addresses are detected.
Syntax	**config gratuitous_arp send send dup_ip_detected [enable | disable]**
Description	The **config gratuitous_arp send send dup_ip_detected** command is used to enable or disable the sending of gratuitous ARP request packets while duplicate IPs are detected. By default, the state is enabled.
Parameters	*enable* − Enable the sending of gratuitous ARP when a duplicate IP is detected. *disable* − Disable the sending of gratuitous ARP when a duplicate IP is detected.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable gratuitous ARP request when a duplicate IP is detected:

```
DES-1210-52/ME:5# config gratuitous_arp send dup_ip_detected
enable
Command: config gratuitous_arp send dup_ip_detected enable



Success!
DES-1210-52/ME:5#
```

config gratuitous_arp learning

Purpose	Used to enable or disable the learning of ARP entries in ARP cache based on the received gratuitous ARP packets.
Syntax	**config gratuitous_arp send learning [enable | disable]**
Description	Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. The **config gratuitous_arp send learning** command is used to enable or disable the learning of ARP entries in ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for. Note that, with gratuitous ARP learning, the system will not learn new entries but only do the update on the ARP table based on the received gratuitous ARP packet. By default, the state is enabled.
Parameters	*enable* − Enable the learning of ARP entries based on received gratuitous ARP packets. *disable* − Disable the learning of ARP entries based on received gratuitous ARP packets.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable learning of ARP entries based on the received gratuitous ARP packets:

```
DES-1210-52/ME:5# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable


Success!
DES-1210-52/ME:5#
```

enable gratuitous_arp log

Purpose	Used to enable the gratuitous ARP log.
Syntax	**enable gratuitous_arp log**
Description	The **enable gratuitous_arp log** command is used to enable gratuitous ARP log states. The Switch can log the IP conflict event to inform the administrator.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the System's interface gratuitous ARP log:

```
DES-1210-52/ME:5# enable gratuitous_arp log
Command: enable gratuitous_arp log


Success!
DES-1210-52/ME:5#
```

disable gratuitous_arp log

Purpose	Used to disable the gratuitous ARP log.
Syntax	**disable gratuitous_arp log**
Description	The **disable gratuitous_arp log** command is used to disable gratuitous ARP log states. The Switch can log the IP conflict event to inform the administrator.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the System's interface gratuitous ARP log:

```
DES-1210-52/ME:5# disable gratuitous_arp log
Command: disable gratuitous_arp log


Success!
```

```
DES-1210-52/ME:5#
```

show gratuitous_arp

Purpose	Used to display the gratuitous ARP configuration.
Syntax	**show gratuitous_arp**
Description	The **show gratuitous_arp** command is used to display the gratuitous ARP configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display gratuitous ARP log and trap states:

```
DES-1210-52/ME:5# show gratuitous_arp
Command: show gratuitous_arp


Send on IPIF status up            : Enabled
Send on Duplicate_IP_Detected : Enabled
Gratuitous ARP Learning           : Enabled

IP Interface Name                              : System
Gratuitous ARP Trap                            : Enabled
Gratuitous ARP Log                             : Disabled
Gratuitous ARP Periodical Send Interval : 0

DES-1210-52/ME:5#
```

config gratuitous_arp send periodically

Purpose	Used to configure the interval for periodical sending of gratuitous ARP request packets.
Syntax	**config gratuitous_arp send periodically ipif <ipif_name 12> interval <integer 0-65535>**
Description	The **config gratuitous_arp send periodically ipif** command is used to configure the interval for periodical sending of gratuitous ARP request packets. By default, the interval is 0.
Parameters	*ipif <ipif_name 12>* - Specifies the IP interface name to be configured. *interval <integer 0-65535>* − Periodically send gratuitous ARP interval time in seconds. 0 means it will not send gratuitous ARP periodically.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure gratuitous ARP intervals for the Switch:

```
DES-1210-52/ME:5# config gratuitous_arp send periodically ipif rrd2 interval 100
```

```
Command: config gratuitous_arp send periodically ipif rrd2 interval 100


Success.
DES-1210-52/ME:5#
```

19

POWER SAVING COMMANDS

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

Command	Parameter
config power_saving mode	[hibernation | led | length_detection | port] [enable | disable]
config power_saving	[hibernation | led [all | <portlist>] | port [all | <portlist>]] [add | delete] time_range1 <range_name 20> time_range2 <range_name 20> {clear_time_range}
show power_saving	{hibernation | led | length_detection | port}

Each command is listed in detail, as follows:

config power_saving mode

Purpose	To configure the power saving mode on the switch.
Syntax	**config power_saving mode [hibernation | led | length_detection | port] [enable | disable]**
Description	The **config power_saving mode** command is used to configure the power saving mode on the switch.
Parameters	*hibernation* – Configure the hibernation state to enable or disable. The default value is disabled. *led* – Configure the led state to enable or disable. The default value is disabled. *length_detection* – Configure the length detection state to enable or disable. The default value is disabled. *port* – Configure ports state to be enabled or disabled. *[enable | disable]* – Enable or disable the power saving feature.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure the power saving mode on the switch:

```
DES-1210-52/ME:5# config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable


Success!
DES-1210-52/ME:5#
```

config power_saving

Purpose	To configure the power saving on the switch.
Syntax	**config power_saving [hibernation | led [all | <portlist>] | port [all**

	| <portlist>]] [add | delete] time_range1 <range_name 20> time_range2 <range_name 20> {clear_time_range}
Description	The **config power_saving** command is used to configure the power saving on the switch.
Parameters	hibernation – Configure the hibernation. *led [all | <portlist>]* – Configure the ports for led. *port* – Configure ports. *[add | delete]* – Add or delete time range for power saving mode. *time_range1 <range_name 20>* – Specifies the time range 1 to be configured. *time_range2 <range_name 20>* – Specifies the time range 2 to be configured. *{clear_time_range}* – Clear the time range setting for power saving on the Switch.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure the power saving on the switch:

```
DES-1210-52/ME:5# config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success.
DES-1210-52/ME:5#
```

show power_saving

Purpose	To display power saving information on the switch.
Syntax	**show power_saving {hibernation | led | length_detection | port | link_detection}**
Description	The **show power_saving** is used to display power saving information.
Parameters	hibernation – Display the hibernation state. *led* – Display the led state. *length_detection* – Display the length detection state. *port* – Display ports state. link_detection – Display link detection state.
Restrictions	None.

Example usage:

To display power saving information on the switch:

```
DES-1210-52/ME:5# show power_saving length_detection
Command: show power_saving length_detection

Length Detection State   : Enabled
DES-1210-52/ME:5#
```

20

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	Parameter
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[ports {<portlist>} | cpu | mem]
clear counters	{ports <portlist>}
save log	
clear log	
show log	{index <indexlist> | module <string 32> | severity [all | information | warning]}
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [informational | warning | all] | facility [local0 | local1| local2 | local3 | local4 | local5 | local6 | local7] | state [enable | disable] | udp_port [514 | <udp_port_number 6000-65535>]}
config syslog host	[all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | state [enable | disable] | udp_port [514 | <udp_port_number 6000-65535>] | ipaddress [<ipaddr> | <ipv6addr>]}
delete syslog host	[<index 1-4> | all]
show syslog host	{<index 1-4>}
cable diagnostic port	[<portlist> | all]
config syslogintimeout	<integer 3-30>
config sysgroupinterval	[<integer 120-1225> | 0]
show log_software_module	

Each command is listed in detail, as follows:

show packet ports

Purpose	To display statistics about the packets sent and received in frames per second by the Switch.
Syntax	**show packet ports <portlist>**

Description	The **show packet ports** command displays statistics about packets sent and received by ports specified in the port list. The results are separated into three tables, labeled A, B, and C in the window below. Table A is relevant to the size of the packets, Table B is relevant to the type of packets and Table C is relevant to the type of frame associated with these packets.
Parameters	<*portlist*> − A port or range of ports whose statistics are to be displayed.
Restrictions	None.

Example usage:

To display the packets analysis for port 1:

```
DES-1210-52/ME:5# show packet ports 1
Command: show packet ports 1

 Port Number : 1
 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	To display the error statistics for a port or a range of ports.
Syntax	**show error ports <portlist>**
Description	The **show error ports** command displays all of the packet error statistics collected and logged by the Switch for a given port list.
Parameters	<*portlist*> − A port or range of ports whose error statistics are to be displayed.
Restrictions	None.

Example usage:

To display the errors of port 2:

```
DES-1210-52/ME:5# show errors port 1
Command: show error ports 1
```

```
Port Number : 1
                 RX Frames                                   TX Frames
------------------                              -------------------
 CRC Error      0               Excessive Deferral    0
 Undersize      0               CRC Error             0
 Oversize       0               Late Collision        0
 Fragment       8               Excessive Collision   0
 Jabber         0               Single Collision      0
 Drop Pkts      0               Collision             0

DES-1210-52/ME:5#
```

show utilization

Purpose	To display real-time port utilization statistics.
Syntax	**show utilization [ports {<portlist>} | cpu | mem]**
Description	The **show utilization** command displays the real-time utilization statistics for ports in bits per second (bps) for the Switch, and for the CPU in percentage.
Parameters	*ports* – Entering this parameter will display the current port utilization of the Switch. *<portlist>* – Specifies a range of ports to be displayed. *cpu* – Entering this parameter will display the current CPU utilization of the Switch. *mem* – Entering this parameter will display the current memory utilization of the Switch.
Restrictions	None.

To display the port 2 utilization statistics:

```
DES-1210-52/ME:5# show utilization ports 2
Command: show utilization ports 2



 Port TX/sec RX/sec Util
 ------ --------   ---------- ----
 2      0        0          0




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

To display the cpu utilization statistics:

```
DES-1210-52/ME:5# show utilization cpu
Command: show utilization cpu

CPU Utilization :
-------------------------------------------------------------------------------
Five Seconds - 1 %   One Minute - 1 %   Five Minutes - 1 %
```

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

clear counters

Purpose	To clear the Switch's statistics counters.
Syntax	**clear counters{ports <portlist>}**
Description	The **clear counters** command clears the counters used by the Switch to compile statistics.
Parameters	*ports <portlist>* - Specifies the counters of ports to be cleared.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To clear the counters:

```
DES-1210-52/ME:5# clear counters



Success.
DES-1210-52/ME:5#
```

save log

Purpose	To save the Switch's history log.
Syntax	**save log**
Description	The **save log** command saves the Switch's history log.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To save the log information:

```
DES-1210-52/ME:5# save log
Command: save log



Success.

DES-1210-52/ME:5#
```

clear log

Purpose	To clear the Switch's history log.

Syntax	**clear log**
Description	The **clear log** command clears 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-1210-52/ME:5# clear log
Command: clear log


Success.
DES-1210-52/ME:5#
```

show log

Purpose	To display the Switch history log.
Syntax	**show log {index <indexlist> | module <string 32> | severity [all | information | warning]}**
Description	The **show log** command displays the contents of the Switch's history log.
Parameters	*index <indexlist>* − The number of entries in the history log to displayed. *module <string 32>* − The module of entries in the history log to be displayed. *[all* | *information* | *warning] -*
Restrictions	None.

Example usage:

To display the Switch history log:

```
DES-1210-52/ME:5# show log
Command: show log

Index  Time                 Log Text
-----  -------------------- ------------------------------------------




DES-1210-52/ME:5#
```

enable syslog

Purpose	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-1210-52/ME:5# enable syslog
Command: enable syslog

Success.

DES-1210-52/ME:5#
```

disable syslog

Purpose	To disable the system log from being sent to a remote host.
Syntax	**disable syslog**
Description	The **disable syslog** command disables the system log from being 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-1210-52/ME:5# disable syslog
Command: disable syslog

Success.

DES-1210-52/ME:5#
```

show syslog

Purpose	To display the syslog protocol status.
Syntax	**show syslog**
Description	The **show syslog** command displays the syslog status (enabled or disabled).
Parameters	None.
Restrictions	None.

Example usage:

To display the current status of the syslog function:

```
DES-1210-52/ME:5# show syslog
Command: show syslog

Syslog Global State: Enabled

DES-1210-52/ME:5#
```

create syslog host

Purpose

To create a new syslog host.

Syntax

create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [informational | warning | all] | facility [local0 | local1| local2 | local3 | local4 | local5 | local6 | local7] | state [enable | disable] | udp_port [514 | <udp_port_number 6000-65535>]}

Description

The **create syslog host** command creates a new syslog host.

Parameters

all − Specifies that the command is to be applied to all hosts.

<index 1-4> − The syslog host index id. There are four available indices, numbered 1 to 4.

ipaddress [<ipaddr> | *<ipv6addr>]* − The IPv4 or IPv6 address of the remote host to which syslog messages are to be sent.

severity − The message severity level indicator. These are described in the table 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 are to be sent to the remote host. This corresponds to number 6 from the list above.

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

all − Specifies that all message are to 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 table below (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)
	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 are to be sent to the remote host. This corresponds to number 16 from the list above. *local1* − Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above. *local2* − Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above. *local3* − Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above. *local4* − Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above. *local5* − Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above. *local6* − Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above. *local7* − Specifies that local use 7 messages is sent to the remote host. This corresponds to number 23 from the list above. *udp_port [514* | *<udp_port_number 6000-65535>]* − Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host. *state [enable* | *disable]* − Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.	
Restrictions	Only Administrator or operator-level users can issue this command.	

Example usage:

To create syslog host:

```
DES-1210-52/ME:5# create syslog host 1 ipaddress 10.90.90.97 severity informational state enable facility local0 udp_port 514

Command: create syslog host 1 ipaddress 10.90.90.97 severity informational state enable facility local0 udp_port 514
```

```
Success.

DES-1210-52/ME:5#
```

config syslog host

Purpose	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] | state [enable | disable] | udp_port [514 | <udp_port_number 6000-65535>] | ipaddress [<ipaddr> | <ipv6addr>]}**
Description	The **config syslog host** command configures the syslog protocol to send system log information to a remote host.
Parameters	*all* − Specifies that the command applies to all hosts. *<index 1-4>* − Specifies that the command applies to an index of hosts. There are four available indices, numbered 1 to 4. *severity* − The message severity level indicator. These are described in the following table (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 are to be sent to the remote host. This corresponds to number 6 from the list above.

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

all − Specifies that all message are to 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)
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 are to be sent to the remote host. This corresponds to number 16 from the list above.

local1 − Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above.

local2 − Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.

local3 − Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.

local4 − Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.

local5 − Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.

local6 − Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.

local7 − Specifies that local use 7 messages are to be sent to the remote host. This corresponds to number 23 from the list above.

udp_port [514 | *<udp_port_number 6000-65535>]* − Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.

ipaddress [<ipaddr> | *<ipv6addr>]* − Specifies the IPv4 or IPv6 address of the remote host to which syslog messages are to 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-1210-52/ME:5# config syslog host 1 severity all facility local0
Command: config syslog host 1 severity all facility local0



Success.

DES-1210-52/ME:5#
```

delete syslog host

Purpose	To remove a previously configured syslog host from the Switch.
Syntax	**delete syslog host [<index 1-4> | all]**
Description	The **delete syslog host** command removes a previously configured syslog host from the Switch.
Parameters	*<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4. *all* − Specifies that the command applies to all hosts.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DES-1210-52/ME:5# delete syslog host all
Command: delete syslog host all

Success.

DES-1210-52/ME:5#
```

show syslog host

Purpose	To display the syslog hosts currently configured on the Switch.
Syntax	**show syslog host {<index 1-4>}**
Description	The **show syslog host** command displays the syslog hosts that are currently configured on the Switch.
Parameters	*<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4.
Restrictions	None.

Example usage:

To show Syslog host information:

```
DES-1210-52/ME:5# show syslog host
Command: show syslog host

Host ID  Host IP Address   Severity    Facility    UDP Port  Status
```

```
---------   ----------------------   -----------   ------------  -------------  -----------
1                      1.1.2.1      All        Local0     514          Enabled

Total Entries : 1


DES-1210-52/ME:5#
```

cable diagnostic port

Purpose	To determine if there are any errors on the copper cables and the position where the errors may have occurred.
Syntax	**cable diagnostic port [<portlist> | all]**
Description	The **cable diagnostic port** command is used to determine if there are any errors on the copper cables and the position where the errors may have occurred. Cable length is detected as following range: <50m, 50~80, 80~100, >100m. Deviation is +/-5 meters, therefore "No Cable" may be displayed under "Test Result," when the cable used is less than 5 m in length. The Fault Distance will show "No Cable", whether the fiber is connected to the port or not.
Parameters	*<portlist>* – A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured.
Restrictions	None.

Example usage:

To determine the copper cables and position of port 3 on the Switch:

```
DES-1210-52/ME:5# cable diagnostic port 3
Command: cable diagnostic port 3

 Perform Cable Diagnostics ...

 Port  Type   Link Status  Test Result   Fault Distance (meters)  Length(M)
 ----   -----    ---------------  -----------------  --------------------------------   ---------
 3      FE      Link Down   Pair1:N/A      Pair1:No Cable            N/A
                            Pair2:OPEN  Pair2:1
                            Pair3:N/A      Pair3:N/A
                            Pair4:N/A      Pair4:N/A

DES-1210-52/ME:5#
```

config syslogintimeout

Purpose	To configure the system login timeout.
Syntax	**config syslogintimeout <integer 3-30>**
Description	The **config syslogintimeout** command is used to configure the system login timeout.
Parameters	*<integer 3-30>* − Specify the system login time. The range is between 3 and 30 minutes.

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

Example usage:

To configure the system login timeout:

```
DES-1210-52/ME:5# config syslogintimeout 30
Command: config syslogintimeout 30



Success.
DES-1210-52/ME:5#
```

config sysgroupinterval

Purpose	To configure the system group interval to optimal frequency.
Syntax	**config sysgroupinterval [<integer 120-1225> | 0]**
Description	The **config sysgroupinterval** command is used to configure the system group interval to optimal frequency.
Parameters	*[<integer 120-1225>* | *0]* − Specify the system group interval. And the range is from 120 to 1225 seconds. 0 means disabling the reporting function.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the system group interval:

```
DES-1210-52/ME:5# config sysgroupinterval 200
Command: config sysgroupinterval 200

DES-1210-52/ME:5#
```

show log_software_module

Purpose	To display the protocols or applications which support the enhanced logs.
Syntax	**show log_software_module**
Description	The **show log_software_module** command is used to display the protocols or applications that support the enhanced logs.
Parameters	None.
Restrictions	None.

Example usage:

To display the protocols or applications that support the enhanced log:

```
DES-1210-52/ME:5# show log_software_module
Command: show log_software_module

CLI    SYSTEM

DES-1210-52/ME:5#
```

21

SPANNING TREE COMMANDS

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

Command	Parameter
config stp	{maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10>}
config stp ports	<portlist> {externalcost [auto | <value 1-200000000>] | edge [auto | true | false] | hellotime <value 1-2> | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable | disable] | migrate [yes | no] | priority <value 0-240> | restricted_role [true | false] | restricted_tcn [true | false] }
config stp version	[mstp | rstp | stp]
config stp fbpdu	[enable | disable]
config stp priority	<value 0-61440> instance_id <value 0-63>
enable stp	
disable stp	
show stp	
show stp ports	{<portlist>}
show stp instance	<value 0-63>}
show stp mst_config_id	
create stp instance_id	<value 1-63>
delete stp instance_id	<value 1-63>
config stp instance_id	<value 1-63> [add_vlan | remove_vlan] <vidlist>
config stp mst_config_id	[revision_level <int 0-65535> | name <string 32>]
config stp mst_ports	<portlist> instance_id <value 0-63> {internalCost [auto | value 1-200000000] | priority <value 0-240>}
config stp trap	{new_root [enable | disable] | topo_change [enable | disable]}

Each command is listed in detail, as follows:

config stp

Purpose	To setup STP, RSTP and MSTP on the Switch.
Syntax	**config stp {maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10>}**
Description	The **config stp** command configures the Spanning Tree Protocol (STP) for the entire switch. All commands here are 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 aids 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 starts sending its own BPDU to all other switches for permission to become the Root Bridge. If your switch has the lowest priority, it becomes the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20. *hellotime <value 1-10>* − The user may set the time interval between transmission of configuration messages by the root device in STP, or by the designated router, thus stating that the Switch is still functioning. The value may be between 1 and 10 seconds. The default value is 2 seconds. *forwarddelay <value 4-30>* − The amount of time (in seconds) that the root device will wait before changing from Blocking to Listening , and from Listening to Learning states. The value may be between 4 and 30 seconds. The default is 15 seconds. *txholdcount <value 1-10>* − The maximum number of BDPU Hello packets transmitted per interval. Default value = 3.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and hellotime 2:

```
DES-1210-52/ME:5# config stp hellotime 2 forwarddelay 4 maxage 6
txholdcount 2
Command: config stp hellotime 2 forwarddelay 4 maxage 6 txholdcount 2



Success.
DES-1210-52/ME:5#
```

config stp ports

Purpose	To setup STP on the port level.
Syntax	**config stp ports <portlist> {externalcost [auto | <value 1-200000000>] | edge [auto | true | false] | hellotime <value 1-2> | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable | disable] | migrate [yes | no] | priority <value 0-240> | restricted_role [true | false] | restricted_tcn [true | false] }**
Description	The **config stp ports** command configures STP for a group of ports.
Parameters	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. *externalCost* − 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* – Automatically sets the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost:10Mbps port = 2000000. 100Mbps port = 200000. Gigabit port = 20000. Port-channel = 20000. • <*value 1-200000000*> - Defines 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. *edge [auto* | *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. The default setting for this parameter is false. *hellotime* <*value 1-2*> – 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 2 seconds. The default is 2 seconds. *p2p [true* | *false* | *auto]* – *true* indicates a point-to-point (P2P) link. 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. (A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port). 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* | *system]* – If enabled - allows the forwarding of STP BPDU packets from other network devices Disable – blocking STP BPDU packets from other network devices. System – indicates that port will behave as global switch's fbpdu value configured. Fbpdu value valid only when STP port state is disabled or global STP state is disabled. The default is system. *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 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 and 802.1D network connects to and 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. *priority* <*value 0-240*> − Specifies the priority. The range is from 0 to 240. *restricted_role [true* | *false]* − To decide if this is to be selected as the Root Port. The default value is false. *restricted_tcn [true* | *false]* − To decide if this port is to propagate topology change. The default value is false.

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

Example usage:

To configure STP with path cost 19 and state enable for ports 1-3:

```
DES-1210-52/ME:5# config stp ports 1-3 externalcost 19 state enable
Command: config stp ports 1-3 externalcost 19 state enable

Success.
DES-1210-52/ME:5#
```

config stp version

Purpose	To globally set the version of STP on the Switch.
Syntax	**config stp version [mstp | rstp | stp]**
Description	The **config stp version** command sets the version of the spanning tree to be implemented on the Switch.
Parameters	*mstp* – Sets the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. *rstp* – Sets the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *stp* – Sets the Spanning Tree Protocol (STP) globally on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-1210-52/ME:5# config stp version mstp
Command: config stp version mstp

Success.
DES-1210-52/ME:5#
```

config stp fbpdu

Purpose	To globally set the fbpdu of STP on the Switch.
Syntax	**config stp fbpdu [enable | disable]**
Description	The **config stp fbpdu** command allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the Switch globally for the Spanning Tree Protocol (STP) fbpdu enable:

```
DES-1210-52/ME:5# config stp fbpdu enable
Command: config stp fbpdu enable

Success.
DES-1210-52/ME:5#
```

config stp priority

Purpose	To update the STP instance configuration.
Syntax	**config stp priority <value 0-61440> instance_id <value 0-63>**
Description	The **config stp priority** command updates the STP instance configuration settings on the Switch. The MSTP uses the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions instructs the Switch to give precedence to the selected instance_id for forwarding packets. A lower value indicates a higher priority.
Parameters	*priority <value 0-61440>* - The priority for a specified *instance_id* for forwarding packets. The value may be between 0 and 61440, and must be divisible by 4096. A lower value indicates a higher priority. *instance_id <value 0-63>* - The value of the previously configured instance id for which the user wishes to set the priority value. An instance_id of 0 denotes the default instance_id (CIST) internally set on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the priority value for instance_id 2 as 4096:

```
DES-1210-52/ME:5# config stp priority 4096 instance_id 2
Command: config stp priority 4096 instance_id 2

Success.

DES-1210-52/ME:5#
```

enable stp

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

Example usage:

To enable STP, globally, on the Switch:

```
DES-1210-52/ME:5# enable stp
Command: enable stp

Success.
DES-1210-52/ME:5#
```

disable stp

Purpose	To globally disable STP on the Switch.

Syntax	**disable stp**
Description	The **disable stp** command sets the Spanning Tree Protocol to be globally disabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DES-1210-52/ME:5# disable stp
Command: disable stp

Success.
DES-1210-52/ME:5#
```

show stp

Purpose	To display the Switch’s current STP configuration.
Syntax	**show stp**
Description	The **show stp** command displays the Switch’s current STP configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the status of STP on the Switch:

```
DES-1210-52/ME:5# show stp
Command: show stp


STP Bridge Global Settings
---------------------------------------------
STP Status              : Enabled
STP Version             : MSTP
Bridge Priority         : 32768
Max Age                 : 6
Hello Time              : 2
Forward Delay           : 4
TX Hold Count           : 2
Forward BPDU            : Enabled
Root Cost               : 0
Root Maximum Age        : 6
Root Forward Delay      : 4
Root Port               : 0
Root Bridge             : 80:00:00:01:02:03:04:05

DES-1210-52/ME:5#
```

show stp ports

Purpose	To display the Switch's current instance_id configuration.
Syntax	**show stp ports {<portlist>}**
Description	The **show stp ports** command displays the STP Instance Settings and STP Instance Operational Status currently implemented on the Switch.
Parameters	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To show stp port 1 on switch one:

```
DES-1210-52/ME:5# show stp ports 1
Command: show stp ports 1



MSTP Port Information
-----------------------------
Port Index:1 ,  Port STP:Enabled ,      P2P:Auto ,
External PathCost : AUTO/200000 ,       Edge Port:Auto ,
Port RestrictedRole:False ,     Port RestrictedTCN:False
Port Priority:128 ,     Port Forward BPDU:Enabled ,
MSTI Designated Bridge         Internal PathCost  Prio   Status       Role
------  --------------------------       ------------------------  ------  ----------       ----------
0      80:00:00:01:02:03:04:05  200000                128    Disabled     Disabled

DES-1210-52/ME:5#
```

show stp instance

Purpose	To display the Switch's STP instance configuration
Syntax	**show stp instance {<value 0-63>}**
Description	The **show stp instance** command displays the Switch's current STP Instance Settings and the STP Instance Operational Status.
Parameters	*<value 0-63>* - The value of the previously configured instance_id on the Switch. The value may be between 0 and 63. An entry of 0 displays 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-1210-52/ME:5# show stp instance 0
Command: show stp instance 0
```

```


 ## MST00
Designated Root Bridge   00:01:02:03:04:05    Priority 32768
                         We are the Root for CST
                         Port 0       ,  path cost 0
Regional Root Bridge     00:01:02:03:04:05    Priority  32768
                         Path cost 0
Designated Bridge        00:01:02:03:04:05    Priority  32768
Configured Forward delay 4, Max age 6, Max hops 20
Operational Forward delay 4, Max age 6

Interface Role        Sts        Cost    Prio.Nbr Type
------------- --------   ---     -------    ------------- ----


DES-1210-52/ME:5#
```

show stp mst_config_id

Purpose	To display the MSTP configuration identification.
Syntax	**show stp mst_config_id**
Description	The **show stp mst_config_id** 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-1210-52/ME:5# show stp mst_config_id
Command: show stp mst_config_id



Name          [00-01-02-03-04-05]
Revision       0
Instance       Vlans mapped
 --------       ----------------------------------------------------
  0          1-1024,1025-2048,2049-3072,3073-4094
 --------------------------------------------------------------------


DES-1210-52/ME:5#
```

create stp instance_id

Purpose	To create instance ID on the Switch.
Syntax	**create stp instance_id <value 1-63>**
Description	The **create stp instance_id** command creates an instance ID of STP on the Switch.

Parameters	*<value 1-63>* - The value of the instance ID to be created.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create instance id 1:

```
DES-1210-52/ME:5# create stp instance_id 1
Command: create stp instance_id 1

Warning: There is no VLAN mapping to this instance_id!

Success.
DES-1210-52/ME:5#
```

delete stp instance_id

Purpose	To delete instance ID on the Switch.
Syntax	**delete stp instance_id <value 1-63>**
Description	The **delete stp instance_id** command removes the instance ID of STP on the Switch.
Parameters	*<value 1-63>* - The value of the instance ID to be removed.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To remove instance id 1:

```
DES-1210-52/ME:5# delete stp instance_id 1
Command: delete stp instance_id 1



Success.
DES-1210-52/ME:5#
```

config stp instance_id

Purpose	To configure instance ID on the Switch.
Syntax	**config stp instance_id <value 1-63> [add_vlan | remove_vlan] <vidlist>**
Description	The **config stp instance_id** 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.
Parameters	*<value 1-63>* − Enter a number between 1 and 63 to define the *instance_id*. The Switch supports 63 STP instances 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-level users can issue this command.

Example usage:

To configure instance ID 1 to add VID 10:

```
DES-1210-52/ME:5# config stp instance_id 1 add_vlan 10
Command: config stp instance_id 1 add_vlan 10




Success.
DES-1210-52/ME:5#
```

config stp mst_config_id

Purpose	To update the MSTP configuration identification.
Syntax	**config stp mst_config_id [revision_level <int 0-65535> | name <string 32>]**
Description	The **config stp mst_config_id** command uniquely identifies the MSTP configuration currently configured on the Switch. Information entered here is attached to BDPU packets as an identifier for the MSTP region to which it belongs. Switches having the same revision_level, name and identical vlans mapped for STP instance_ids are considered to be part of the same MSTP region.
Parameters	*revision_level <int 0-65535>*– The MSTP configuration revision number. The value may be between 0 and 65535. This value, along with the name and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. The default setting is 0. *name <string 32>* - A string of up to 32 alphanumeric characters to uniquely identify the MSTP region on the Switch. This name, along with the revision_level value and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. If no name is entered, the default name is the MAC address of the device.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the MSTP region of the Switch with revision_level 10:

```
DES-1210-52/ME:5# config stp mst_config_id revision_level 10
Command: config stp mst_config_id revision_level 10




Success.
DES-1210-52/ME:5#
```

config stp mst_ports	
Purpose	To update the port configuration for a MSTP instance.
Syntax	**config stp mst_ports <portlist> instance_id <value 0-63> {internalCost [auto | value 1-200000000] | priority <value 0-240>}**
Description	The **config stp mst_ports** command updates the port configuration for a STP instance_id. If a loop occurs, the MSTP function uses the port cost to select an interface to put into the forwarding state (if the switch isn't Root). If the switch is Root, then higher priority value for interfaces will influence on selected ports to be forwarding first at connected network devices. In instances where the priority value is identical, the MSTP function implements the lowest port number into the forwarding state and other interfaces are blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. *instance_id <value 0-63>* - The value may be between 0 and 63. An entry of 0 denotes the CIST (Common and Internal Spanning Tree. *internalCost* – The relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. The default setting is auto. There are two options: • *auto* – Specifies setting the quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • *value 1-200000000* – Specifies setting the quickest route when a loop occurs. The value may be in the range of 1-200000000. A lower internalCost represents a quicker transmission. *priority <value 0-240>* - The priority for the port interface The value may be between 0 and 240. A lower number denotes a higher priority. A higher priority designates the interface to forward packets first.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-1210-52/ME:5# config stp mst_ports 6-8 instance_id 1 internalCost auto
priority 16
Command: config stp mst_ports 6-8 instance_id 1 internalCost auto priority 16



Success.
DES-1210-52/ME:5#
```

config stp trap	
Purpose	To configure the sending state for STP traps.
Syntax	**config stp trap {new_root [enable | disable] | topo_change [enable | disable]}**
Description	The **config stp mst_ports** command is used to configure the sending state for STP traps.
Parameters	*new_root [enable* | *disable]* – Enable or disable sending of new root trap. The default state is enabled. *topo_change [enable* | *disable]* – Enable or disable sending of topology change trap. The default state is enabled.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure the new root and topo change to be enabled for STP trap:

```
DES-1210-52/ME:5# config stp trap new_root disable topo_change enable
Command: config stp trap new_root disable topo_change enable



Success.
DES-1210-52/ME:5#
```

22

FORWARDING DATABASE COMMANDS

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

Command	Parameter
create fdb	<vlan_name 32> <macaddr> port <port 1-52>
create multicast_fdb	<int 1-4094><macaddr>
config multicast_fdb	<integer 1-4094> <macaddr> [add | delete] <portlist>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
enable flood_fdb	
disable flood_fdb	
config flood_fdb	[log | trap] [enable | disable]
show flood_fdb	
clear flood_fdb	
show flow_meter	{profile_id <value 1-10> | access_id <value 1-128>}
show fdb	{port <port 1-52> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}
config multicast filter	<portlist> [forward | filter]
show multicast filter port_mode	
create auto_fdb	<ipaddr>
delete auto_fdb	<ipaddr>
show auto_fdb	{<ipaddr>}

Each command is listed in detail, as follows:

create fdb	
Purpose	To create a static entry in the unicast MAC address forwarding table (database)
Syntax	**create fdb <vlan_name 32> <macaddr> port <port 1-52>**
Description	The **create fdb** command creates a static entry in 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 to be added to the forwarding table.

	port <port 1-52> − 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-1210-52/ME:5# create fdb default 00-00-00-00-01-02 port 2
Command: create fdb default 00-00-00-00-01-02 port 2

Success.
DES-1210-52/ME:5#
```

create multicast_fdb

Purpose	To create a static entry in the multicast MAC address forwarding table (database).
Syntax	**create multicast_fdb <int 1-4094> <macaddr>**
Description	The **create multicast_fdb** command creates a static entry in the multicast MAC address forwarding table (database).
Parameters	*<integer 1-4094>* − The item of the VLAN on which the MAC address resides. The range is between 1 and 4094. *<macaddr>* − The MAC address to 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-1210-52/ME:5# create multicast_fdb 1 00-00-00-01-02-03
Command: create multicast_fdb 1 00-00-00-01-02-03

Success.
DES-1210-52/ME:5#
```

config multicast_fdb

Purpose	To configure the Switch's multicast MAC address forwarding database.
Syntax	**config multicast_fdb <integer 1-4094> <macaddr> [add | delete] <portlist>**
Description	The **config multicast_fdb** command configures the multicast MAC address forwarding table.
Parameters	*<integer 1-4094>* − The item of the VLAN on which the MAC address resides. The range is between 1 and 4094. *<macaddr>* − The MAC address to be configured to the forwarding table. *add* − Specifies that the MAC address is to be added to the forwarding table. Delete will remove the MAC address from the forwarding table. *delete* − Specifies that the MAC address is to be removed from the

	forwarding table. *<portlist>* − A port or range of ports to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure multicast MAC forwarding:

```
DES-1210-52/ME:5# config multicast_fdb 1 00-00-00-01-02-03
Command: config multicast_fdb 1 00-00-00-01-02-03

Success.

DES-1210-52/ME:5#
```

config fdb aging_time

Purpose	To set the aging time of the forwarding database.
Syntax	**config fdb aging_time <sec 10-1000000>**
Description	The **config fdb aging_time** command sets the aging time of the forwarding database. 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 0 to 630 minutes with a default value of 5 minutes. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the Switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a Switch.
Parameters	*<sec 10-1000000>* − The aging time for the MAC address forwarding database value, in seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To set the fdb aging time:

```
DES-1210-52/ME:5# config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-1210-52/ME:5#
```

delete fdb

Purpose	To delete an entry in the Switch's forwarding database.
Syntax	**delete fdb <vlan_name 32> <macaddr>**
Description	The **delete fdb** command deletes an entry in 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 to be removed from the forwarding table.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DES-1210-52/ME:5# delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.
DES-1210-52/ME:5#
```

enable flood_fdb

Purpose	To enable the Switch’s forwarding database on the Switch.
Syntax	**enable flood_fdb**
Description	The **enable flood_fdb** command enables dynamically learned entries from the Switch’s forwarding database.34
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable FDB dynamic entries:

```
DES-1210-52/ME:5# enable flood_fdb
Command: enable flood_fdb


Success.
DES-1210-52/ME:5#
```

disable flood_fdb

Purpose	To disable the Switch’s forwarding database on the Switch.
Syntax	**disable flood_fdb**
Description	The **disable flood_fdb** command disables dynamically learned entries from the Switch’s forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable FDB dynamic entries:

```
DES-1210-52/ME:5# disable flood_fdb
Command: disable flood_fdb


Success.
```

```
DES-1210-52/ME:5#
```

config flood_fdb

Purpose	To configure the Switch's forwarding database on the Switch.
Syntax	**config flood_fdb [log | trap] [enable | disable]**
Description	The **config flood_fdb** command configures dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure FDB dynamic entries:

```
DES-1210-52/ME:5# config flood_fdb trap disable log enable
Command: config flood_fdb trap disable log enable



Success.
DES-1210-52/ME:5#
```

show flood_fdb

Purpose	To display the Switch's forwarding database on the Switch.
Syntax	**show flood_fdb**
Description	The **show flood_fdb** command displays dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	None.

Example usage:

To display FDB dynamic entries:

```
DES-1210-52/ME:5# show flood_fdb
Command: show flood_fdb

Flooding FDB State : Enabled
Log State          : Disabled
Trap State         : Disabled

Value  VLAN ID   MAC Address        Time stamp
--------- ------------   -------------------        ------------------


DES-1210-52/ME:5#
```

clear flood_fdb

Purpose	To clear the Switch's forwarding database of all dynamically learned MAC addresses.

Syntax	**clear flood_fdb**
Description	The **clear flood_fdb** command clears dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

```
DES-1210-52/ME:5# clear flood_fdb
Command: clear flood_fdb

Success.
DES-1210-52/ME:5#
```

show flow_meter

Purpose	To display the flow meter information on the Switch.
Syntax	**show flow_meter {profile_id <value 1-10> | access_id <value 1-128>}**
Description	The **show flow_meter** command displays the flow meter information on the Switch.
Parameters	*profile_id <value 1-10>* - .Specify the profile id to be displayed. *access_id <value 1-128>* - Specify the access id to be displayed.
Restrictions	None.

Example usage:

To display flow meter information:

```
DES-1210-52/ME:5# show flow_meter
Command: show flow_meter


Flow Meter information:
------------------------------------
Total Flow Meter Entries: 0

DES-1210-52/ME:5#
```

show multicast_fdb

Purpose	To display the contents of the Switch's multicast forwarding database.
Syntax	**show multicast_fdb {vlan <vlan_name 32> | mac_address <macaddr>}**
Description	The **show multicast_fdb** command displays the current contents of the Switch's multicast MAC address forwarding database.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN on which the MAC address resides. *mac_address <macaddr>* − The MAC address that will be added to

	the forwarding table.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To display multicast MAC address table:

```
DES-1210-52/ME:5# show multicast_fdb
Command: show multicast_fdb

Static Multicast Table
-----------------------------------

Total Mac Addresses displayed: 0

DES-1210-52/ME:5#
```

show fdb	
Purpose	To display the current unicast MAC address forwarding database.
Syntax	**show fdb {port <port 1-52> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}**
Description	The **show fdb** command displays the current contents of the Switch's forwarding database.
Parameters	*<port 1-52>* − The port number corresponding to the MAC destination address. The Switch always forwards 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 entry in the forwarding table. *static* − Specifies that static MAC address entries are to be displayed. *aging_time* − Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DES-1210-52/ME:5# show fdb
Command: show fdb


VID  VLAN Name                MAC Address        Port   Type
---- ------------------------------ -------------------------- ------    -------------------
1    default                 00-01-02-03-04-05   CPU   Self



Total Entries  : 1

DES-1210-52/ME:5#
```

To display the aging time:

```
DES-1210-52/ME:5# show fdb aging_time
Command: show fdb aging_time

Unicast MAC Address Aging Time = 300 (seconds)

DES-1210-52/ME:5#
```

config multicast filter

Purpose	To configure multicast filtering.
Syntax	**config multicast filter <portlist> [forward | filter]**
Description	The **config multicast filtering_mode** command enables filtering of multicast addresses.
Parameters	*<portlist>* - A port or range of ports to be configured. *forward* - Forwards unregistered multicast packets. *filter* - Filter unregistered multicast packets.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure multicast filtering

```
DES-1210-52/ME:5# config multicast filter 3-5 forward
Command: config multicast filter 3-5 forward

Success.
DES-1210-52/ME:5#
```

show multicast filter port_mode

Purpose	To display multicast filtering settings on the Switch.
Syntax	**show multicast filter port_mode**
Description	The **show multicast filter port_mode** command displays the multicast filtering settings.
Parameters	None.
Restrictions	None.

Example usage:

To show multicast filtering settings:

```
DES-1210-52/ME:5# show multicast filter port_mode
Command: show multicast filter port_mode

 Port     Multicast Filtering Mode
------   ------------------------------------------


   1    Forward Unregistered Groups
   2    Forward Unregistered Groups
   3    Forward Unregistered Groups
   4    Forward Unregistered Groups
```

```
  5    Forward Unregistered Groups
  6    Forward Unregistered Groups
  7    Forward Unregistered Groups
  8    Forward Unregistered Groups
  9    Forward Unregistered Groups
 10    Forward Unregistered Groups
 11    Forward Unregistered Groups
 12    Forward Unregistered Groups
 13    Forward Unregistered Groups
 14    Forward Unregistered Groups
 15    Forward Unregistered Groups
 16    Forward Unregistered Groups
 17    Forward Unregistered Groups
 18    Forward Unregistered Groups
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

create auto_fdb	
Purpose	To create a static entry in the auto forwarding table (database).
Syntax	**create auto_fdb <ipaddr>**
Description	The **create auto_fdb** command creates a static entry in the multicast MAC address forwarding table (database).
Parameters	*<ipaddr>* − The IP address to be added to the auto forwarding table.
Restrictions	None.

Example usage:

To create auto forwarding table:

```
DES-1210-52/ME:5# create auto_fdb 172.21.47.13
Command: create auto_fdb 172.21.47.13

Success.
DES-1210-52/ME:5#
```

delete auto_fdb	
Purpose	To delete a static entry in the auto forwarding table (database).
Syntax	**delete auto_fdb <ipaddr>**
Description	The **delete auto_fdb** command removes a static entry in the multicast MAC address forwarding table (database).
Parameters	*<ipaddr>* − The IP address to be deleted from the auto forwarding table.
Restrictions	None.

Example usage:

To delete auto forwarding table:

```
DES-1210-52/ME:5# delete auto_fdb 172.21.47.13
Command: delete auto_fdb 172.21.47.13
```

```
Success.
DES-1210-52/ME:5#
```

show auto_fdb

Purpose	To display a static entry in the auto forwarding table (database).
Syntax	**show auto_fdb {<ipaddr>}**
Description	The **show auto_fdb** command displays a static entry in the multicast MAC address forwarding table (database).
Parameters	*<ipaddr>* − The IP address to be display from the auto forwarding table.
Restrictions	None.

Example usage:

To display auto forwarding table:

```
DES-1210-52/ME:5# show auto_fdb
Command: show auto_fdb

IP Address      VLAN ID   MAC Address       Port   Time Stamp
----------------     -------------- ----------------------     ------    -------------------
172.21.47.13

Success.
DES-1210-52/ME:5#
```

23
BROADCAST STORM CONTROL COMMANDS

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

Command	Parameter
config traffic control	[<portlist> | all] {[action [drop | shutdown] | countdown [0 | <minutes 5-30>] | broadcast | multicast | unicast | threshold <value 0- 1024000> | time_interval <time_interval 5-30>]} [enable | disable]
config traffic control auto_recover_time	[0 | <min 1-65535>]
show traffic control	{<portlist>}
config traffic trap	[storm_cleared | storm_occured | both | none]

Each command is listed in detail, as follows:

config traffic control

Purpose	To configure broadcast / multicast / unknown unicast traffic control.
Syntax	**config traffic control [<portlist> | all] {[action [drop | shutdown] | countdown [0 | <minutes 5-30>] | broadcast | multicast | unicast | threshold <value 0 - 1024000> | time_interval <time_interval 5-30>]} [enable | disable]**
Description	The **config traffic control** command configures broadcast, multicast and unknown unicast storm control.
Parameters	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *action [drop* | *shutdown]* − Specifies the traffic control action to be drop or shutdown. A traffic control trap is active only when the control action is configured as “shutdown”. If the control action is “drop”, there will no traps issue while storm event is detected. *countdown [0* | *<minutes 5-30>]* − Specifies the countdown time of traffic control. *storm_type* – The type of broadcast storm for which to configure the traffic control. The options are: • *broadcast* – Enables broadcast storm control only. • *multicast* – Enables broadcast and multicast storm control. • *unicast* – Enables broadcast and unicast storm control. *threshold <value 0-1024000>* − The upper threshold at which the specified traffic control is switched on. The value is the number of broadcast/multicast/dlf packets, in Kbps, received by the Switch that will trigger the storm traffic control measures. The value ranges in size from 0 to 1024000 Kbps. The default setting is 64 Kbit/sec. *<time_interval 5-30>* − Specifies the time interval of traffic control. *[enable* | *disable]* – Enables or disables the specified storm type.

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

Example usage:

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

```
DES-1210-52/ME:5# config traffic control all multicast enable unicast disable
broadcast enable threshold 64
Command: config traffic control all multicast enable unicast disable broadcast e
nable threshold 64

*Note: Setting count down for drop mode port was ignored.
Success.

DES-1210-52/ME:5#
```

config traffic control auto_recover_time

Purpose	To configure the traffic auto recover time that allowed for a port to recover from shutdown forever status.
Syntax	**config traffic control auto_recover_time [0 | <min 1-65535>]**
Description	The **config traffic control auto_recover_time** command configures.
Parameters	*[0 | <min 1-65535>]* – Specifies the automatic recovery time to be used. The value must be between 1 and 65535 minutes. 0 means 'no recovery mode'.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the auto recover time to 100:

```
DES-1210-52/ME:5# config traffic control auto_recover_time 100
Command: config traffic control auto_recover_time 100

Success.

DES-1210-52/ME:5#
```

show traffic control

Purpose	To display current traffic control settings.
Syntax	**show traffic control {<portlist>}**
Description	The **show traffic control** command displays the current storm traffic control configuration on the Switch.
Parameters	*<portlist>* - A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display traffic control setting for ports 1-3:

```
DES-1210-52/ME:5# show traffic control 1-3
```

```
Command: show traffic control 1-3

Traffic Storm Control Trap : [None]

Port Thres   Broadcast Multicast Unicast  Action   Count    Time
     hold    Storm     Storm     Storm             down     Interval
---- ------- --------- --------- -------- -------- -------- -----------
1    64      Enabled   Enabled   Disabled Drop     0        0
2    64      Enabled   Enabled   Disabled Drop     0        0
3    64      Enabled   Enabled   Disabled Drop     0        0


Total Entries : 3

DES-1210-52/ME:5#
```

config traffic trap

Purpose	To configure the traffic control trap on the Switch.
Syntax	**config traffic trap [storm_cleared | storm_occured | both | none]**
Description	The **config traffic trap** command configures the current storm traffic trap configuration on the Switch.
Parameters	*storm_cleared* – A notification will be generated when a storm event is cleared. *storm_occured* – A notification will be generated when a storm event is detected. *both* – A notification will be generated both when a storm event is detected and cleared. *none* – No notification will be generated when storm event is detected or cleared.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure traffic trap setting:

```
DES-1210-52/ME:5# config traffic trap both
Command: config traffic trap both

Success.

DES-1210-52/ME:5#
```

24

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	Parameter
enable password_recovery	
disable password_recovery	
show password_recovery	

Each command is listed in detail, as follows:

enable password_recovery	
Purpose	To enable the password recovery mode on the Switch.
Syntax	**enable password_recovery**
Description	The **enable password_recovery** command is used to enable the password recovery mode on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the password recovery mode :

```
DES-1210-52/ME:5# enable password_recovery
Command: enable password_recovery

Success.

DES-1210-52/ME:5#
```

disable password_recovery	
Purpose	To disable the password recovery mode on the Switch.
Syntax	**disable password_recovery**
Description	The **disable password_recovery** command is used to disable the password recovery mode on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable the password recovery mode:

```
DES-1210-52/ME:5# disable password_recovery
Command: disable password_recovery

Success.

DES-1210-52/ME:5#
```

show password_recovery

Purpose	To show the password recovery mode on the Switch.
Syntax	**show password_recovery**
Description	The **show password_recovery** command is used to display the password recovery mode on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the password recovery mode:

```
DES-1210-52/ME:5# show password_recovery
Command: show password_recovery

Password Recovery Mode : Enabled

DES-1210-52/ME:5#
```

25

QOS COMMANDS

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

Command	Parameter
config scheduling	<class_id 0-7> weight <value 1-55>
show scheduling	
config bandwidth_control	[<portlist> | all] {rx_rate [no_limit | <value 63-1000000>] | tx_rate [no_limit | <value 63-1000000>]}
show bandwidth_control	{[<portlist> | all]}
config cos mac_mapping	destination_addr <macaddr> class <class_id 0-3>
show cos mac_mapping	{destination_addr <macaddr>}
delete cos mac_mapping	destination_addr <macaddr>
config cos ip_mapping	destination_ip <ipaddr> class <class_id 0-3>
show cos ip_mapping	{destination_ip <ipaddr>}
delete cos ip_mapping	destination_ip <ipaddr>
config cos ipv6_mapping	destination_ipv6 <ipv6addr> class <class_id 0-3>
show cos ipv6_mapping	{destination_ipv6 <ipv6addr>}
delete cos ipv6_mapping	destination_ipv6 <ipv6addr>
config cos ipv6_tc_mapping	trafficclass <class_id 0-255> class <class_id 0-3>
delete cos ipv6_tc_mapping	trafficclass <class_id 0-255>
show cos ipv6_tc_mapping	{trafficclass <class_id 0-255>}
config cos mapping	port [<portlist> | all] [802.1p | dscp_tos | none]
show cos mapping	{port <portlist>}
config cos protocol_mapping	protocol <ip_protocol 1-255> class <class_id 0-3>
show cos protocol_mapping	{protocol <ip_protocol 1-255>}
delete cos	protocol <ip_protocol 1-255>

Command	Parameter
protocol_mapping	
config cos vlanid_mapping	vid <vlanid 1-4094> class <class_id 0-3>
show cos vlanid_mapping	{vid <vlanid 1-4094>}
delete cos vlanid_mapping	vid <vlanid 1-4094>
config cos tos value	<value 0-7> class <priority 0-7>
show cos tos	{value <value 0-7>}
config cos tcp_port_mapping	destination_port <value 0-65535> class <class_id 0-3>
show cos tcp_port_mapping	{destination_port <value 0-65535>}
delete cos tcp_port_mapping	destination_port <value 0-65535>
config cos udp_port_mapping	destination_port <value 0-65535> class <class_id 0-3
show cos udp_port_mapping	{destination_port <value 0-65535>}
delete cos udp_port_mapping	destination_port <value 0-65535>
config 802.1p user_priority	<priority 0-7> <class_id 0-7>
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> | all] <priority 0-7>
show 802.1p default_priority	{<portlist>}
config scheduling_mechanism	[strict | wrr]
show scheduling_mechanism	
config dscp mode	
config dscp_mapping	dscp_value <value 0-63> class <class_id 0-3>
show dscp_mapping	{dscp_value <value 0-63>}

Each command is listed in detail, as follows:

config scheduling	
Purpose	To configure traffic scheduling for each of the Switch’s QoS queues.

Syntax	**config scheduling <class_id 0-7> weight <value 1-55>**
Description	The **config scheduling** command configures traffic scheduling for each of the Switch's QoS queues. The Switch contains four hardware classes of service. Incoming packets must be mapped to one of these four hardware queues. This command is used to specify the rotation by which these four hardware queues are emptied. The Switch's default (if the **config scheduling** command is not used) is to empty the hardware queues in order – from the highest priority queue (hardware class 3) to the lowest priority queue (hardware class 0). Each hardware queue transmits all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received. The max_packets parameter allows the user to specify the maximum number of packets a given hardware priority queue can transmit before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 15 can be specified. For example, if a value of 3 is specified for all the queues, then the highest hardware priority queue (number 3) will be allowed to transmit 3 packets – then the next lowest hardware priority queue (number 2) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat.
Parameters	*<class_id 0-7>* − The hardware classes of service to which the config scheduling command is to be applied. The four hardware classes of service are identified by number (from 0 to 3) with class 3 having the highest priority. *weight <value 1-55>* − Specifies the weight of packets the above specified priority class of service is allowed to transmit before allowing the next lower priority class of service to transmit its packets. The value may be between 0 and 55. The default value is 1 for *class_id* 0, 2 for *class_id* 1, 4 for *class_id* 2, and 8 for *class_id* 3.
Restrictions	Only administrator or operator-level users can issue this command. This command is usable only if the device was configured to work in round robin scheduling (config scheduling_mechnism)

Example usage:

To configure traffic scheduling:

```
DES-1210-52/ME:5# config scheduling 1 weight 10
Command: config scheduling 1 weight 10

Success.

DES-1210-52/ME:5#
```

show scheduling

Purpose	To display the currently configured traffic scheduling on the Switch.
Syntax	**show scheduling**
Description	The **show scheduling** command displays the current configuration for the maximum number of packets (*max_packet*) value assigned to

	the four priority classes of service on the Switch. The Switch empties the four hardware queues in order, from the highest priority (class 3) to the lowest priority (class 0).
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```
DES-1210-52/ME:5# show scheduling
Command: show scheduling


QOS Output Scheduling

Class ID   Weight
------------  ----------
Class-0    strict
Class-1    strict
Class-2    strict
Class-3    strict
Class-4    strict
Class-5    strict
Class-6    strict
Class-7    strict

DES-1210-52/ME:5#
```

config bandwidth_control

Purpose	To configure bandwidth control on the Switch.
Syntax	**config bandwidth control [<portlist> | all] {rx_rate [no_limit | <value 63-1000000>] | tx_rate [no_limit | <value 63-1000000>]}**
Description	The **config bandwidth_control** command defines bandwidth control.
Parameters	*portlist* - A port or range of ports to be configured. *all* - Specifies that the **config bandwidth_control** command applies to all ports on the Switch. *rx_rate* - Enables ingress rate limiting • *no_limit* – Indicates no limit is defined*.* • <*value 63–1000000*>] – Indicates a range between 63-1000000 kbps. *tx_rate* – Enables egress rate limiting. • *no_limit* – Indicates no limit is defined. • <*value 63–1000000>]* – Indicates a range between 63-1000000 kbps**.**
Restrictions	Only administrator-level users can issue this command.

Example usage:

T o configure bandwidth control configuration:

```
DES-1210-52/ME:5# config bandwidth_control all rx_rate 100 tx_rate
no_limit    Command: config bandwidth_control all rx_rate 100 tx_rate
no_limit



Success.

DES-1210-52/ME:5#
```

show bandwidth_control

Purpose	To display bandwidth control settings on the Switch.
Syntax	**show bandwidth control {[<portlist> | all]}**
Description	The **show bandwidth_control** command displays bandwidth control.
Parameters	<*portlist*> – A port or range of ports to be configured. *all* – Specifies that the **show bandwidth_control** command applies to all ports on the Switch.
Restrictions	None.

Example usage:

T o display the bandwidth control configuration:

```
DES-1210-52/ME:5# show bandwidth_control
Command: show bandwidth_control


Port  RX Rate     Tx Rate     Effective Rx      Effective Tx
      (Kbit/sec)  (Kbit/sec)  (Kbit/sec)        (Kbit/sec)
-----  -------------    ------------- -----------------    -------------------

Total entries : 0
DES-1210-52/ME:5#
```

config cos mac_mapping

Purpose	To configure the CoS MAC mapping method.
Syntax	**config cos mac_mapping destination_addr <macaddr> class <class_id 0-3>**
Description	The **config cos mac_mapping** command is used to configure the CoS MAC mapping method on the Switch.
Parameters	<*macaddr*> - Specifies the MAC address to be mapped. For example, 01:00:5E:00:00:00. <*class_id 0-3*> - Specifies the number of the Switch's hardware priority queue.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the CoS mac mapping on the Switch:

```
DES-1210-52/ME:5# config cos mac_mapping destination_addr 00-00-00-
01-02-03 class 2
Command: config cos mac_mapping destination_addr 00-00-00-01-02-03
class 2



Success.

DES-1210-52/ME:5#
```

show cos mac_mapping

Purpose	To display the CoS MAC mapping method.
Syntax	**show cos mac_mapping {destination_addr <macaddr>}**
Description	The **show cos mac_mapping** command is used to display the CoS MAC mapping method on the Switch.
Parameters	*<macaddr>* - Specifies the MAC address to be removed.
Restrictions	None.

Example usage:

To display the CoS mac mapping on the Switch:

```
DES-1210-52/ME:5# show cos mac_mapping
Command: show cos mac_mapping

MAC ADDRESS              Class
--------------------------------------------------
00-00-00-01-02-03          2



DES-1210-52/ME:5#
```

delete cos mac_mapping

Purpose	To remove the CoS MAC mapping method.
Syntax	**delete cos mac_mapping destination_addr <macaddr>**
Description	The **delete cos mac_mapping** command is used to delete the CoS MAC mapping method on the Switch.
Parameters	*<macaddr>* - Specifies the MAC address to be removed.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the CoS mac mapping on the Switch:

```
DES-1210-52/ME:5# delete cos mac_mapping destination_addr 00-00-00-
01-02-03
Command: delete cos mac_mapping destination_addr 00-00-00-01-02-03



Success.
```

```

DES-1210-52/ME:5#
```

config cos ip_mapping

Purpose	To configure the CoS IP mapping method.
Syntax	**config cos ip_mapping destination_ip <ipaddr> class <class_id 0-3>**
Description	The **config cos ip_mapping** command is used to configure the CoS IP mapping method on the Switch.
Parameters	<*ipaddr*> - Specifies the IP address to be mapped. For example, 10.90.90.99. <*class_id 0-3*> - Specifies the number of the Switch's hardware priority queue.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the CoS IP mapping on the Switch:

```
DES-1210-52/ME:5# config cos ip_mapping destination_ip 10.90.90.96 class 1
Command: config cos ip_mapping destination_ip 10.90.90.96 class 1



Success.

DES-1210-52/ME:5#
```

show cos ip_mapping

Purpose	To display the CoS IP mapping method.
Syntax	**show cos ip_mapping {destination_ip <ipaddr>}**
Description	The **show cos ip_mapping** command is used to display the CoS MAC mapping method on the Switch.
Parameters	<*ipaddr*> - Specifies the IP address to be displayed. For example, 10.90.90.99.
Restrictions	None.

Example usage:

To display the CoS ip mapping on the Switch:

```
DES-1210-52/ME:5# show cos ip_mapping
Command: show cos ip_mapping

IP ADDRESS               Class
--------------------------------
10.90.90.96             1



DES-1210-52/ME:5#
```

delete cos ip_mapping

Purpose	To remove the CoS IP mapping method.
Syntax	**delete cos ip_mapping destination_ip <ipaddr>**
Description	The **delete cos ip_mapping** command is used to delete the CoS IP mapping method on the Switch.
Parameters	*<ipaddr>* - Specifies the IP address to be removed.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the CoS ip mapping on the Switch:

```
DES-1210-52/ME:5# delete cos ip_mapping destination_ip 10.90.90.96
Command: delete cos ip_mapping destination_ip 10.90.90.96



Success!

DES-1210-52/ME:5#
```

config cos ipv6_mapping

Purpose	To configure the CoS IPv6 mapping method.
Syntax	**config cos ipv6_mapping destination_ipv6 <ipv6addr> class <class_id 0-3>**
Description	The **config cos ipv6_mapping** command is used to configure the CoS IPv6 mapping method on the Switch.
Parameters	*<iv6paddr>* - Specifies the IPv6 address to be mapped. For example, 3000::1. *<class_id 0-3>* - Specifies the number of the Switch's hardware priority queue.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the CoS IPv6 mapping on the Switch:

```
DES-1210-52/ME:5# config cos ipv6_mapping destination_ipv6 3000::1 class 1
Command: config cos ipv6_mapping destination_ipv6 3000::1 class 1



Success.

DES-1210-52/ME:5#
```

show cos ipv6_mapping

Purpose	To display the CoS IPv6 mapping method.
Syntax	**show cos ipv6_mapping {destination_ipv6 <ipv6addr>}**

Description	The **show cos ipv6_mapping** command is used to display the CoS MAC mapping method on the Switch.
Parameters	<*ipv6addr*> - Specifies the IPv6 address to be displayed. For example, 3000::1.
Restrictions	None.

Example usage:

To display the CoS ipv6 mapping on the Switch:

```
DES-1210-52/ME:5# show cos ipv6_mapping
Command: show cos ipv6_mapping

IPv6 ADDRESS              Class
-----------------------------------------------
3000::1                    1



DES-1210-52/ME:5#
```

delete cos ipv6_mapping

Purpose	To remove the CoS IPv6 mapping method.
Syntax	**delete cos ipv6_mapping destination_ipv6 <ipv6addr>**
Description	The **delete cos ipv6_mapping** command is used to delete the CoS IPv6 mapping method on the Switch.
Parameters	<*ipv6addr*> - Specifies the IPv6 address to be removed.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the CoS ipv6 mapping on the Switch:

```
DES-1210-52/ME:5# delete cos ipv6_mapping destination_ipv6 3000::1
Command: delete cos ipv6_mapping destination_ipv6 3000::1



Success.

DES-1210-52/ME:5#
```

config cos ipv6_tc_mapping

Purpose	To configure the CoS IPv6 TC mapping method.
Syntax	**config cos ipv6_tc_mapping trafficclass <class_id 0-255> class <class_id 0-3>**
Description	The **config cos ipv6_tc_mapping** command is used to configure the CoS IPv6 mapping method on the Switch.
Parameters	*trafficclass <class_id 0-255>*> - Specifies the IPv6 traffic class to be mapped. The range is 0 to 255. <*class_id 0-3*> - Specifies the number of the Switch’s hardware priority queue.

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

Example usage:

To configure the CoS IPv6 TC mapping on the Switch:

```
DES-1210-52/ME:5# config cos ipv6_tc_mapping trafficclass 1 class 2
Command: config cos ipv6_tc_mapping trafficclass 1 class 2



Success.

DES-1210-52/ME:5#
```

delete cos ipv6_tc_mapping

Purpose	To remove the CoS IPv6 mapping method.
Syntax	**delete cos ipv6_tc_mapping trafficclass <class_id 0-255>**
Description	The **delete cos ipv6_tc_mapping** command is used to delete the CoS IPv6 TC mapping method on the Switch.
Parameters	*trafficclass <class_id 0-255>>* - Specifies the IPv6 TC mapping traffic class to be removed.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the CoS ipv6 TC mapping on the Switch:

```
DES-1210-52/ME:5# delete cos ipv6_tc_mapping trafficclass 1
Command: delete cos ipv6_tc_mapping trafficclass 1



Success.

DES-1210-52/ME:5#
```

show cos ipv6_tc_mapping

Purpose	To display the CoS IPv6 mapping method.
Syntax	**show cos ipv6_tc_mapping {trafficclass <class_id 0-255>}**
Description	The **show cos ipv6_tc_mapping** command is used to delete the CoS IPv6 TC mapping method on the Switch.
Parameters	*trafficclass <class_id 0-255>>* - Specifies the IPv6 TC mapping traffic class to be removed.
Restrictions	None.

Example usage:

To display the CoS ipv6 TC mapping on the Switch:

```
DES-1210-52/ME:5# show cos ipv6_tc_mapping trafficclass 10
Command: show cos ipv6_tc_mapping trafficclass 10

IPv6 Traffic TC          Class
```

```
--------------------------------


DES-1210-52/ME:5#
```

config cos mapping

Purpose	To configure the method of which incoming packets will be identified for the CoS to port mapping feature.
Syntax	**config cos mapping port [<portlist> | all] [802.1p | dscp_tos | none]**
Description	The **config cos mapping port** command is used to configure the method of which incoming packets will be identified for the CoS to port mapping feature on the Switch.
Parameters	*<portlist>* - A port or range of ports to be configured. *all* - Specifies all ports to be configured on the Switch. *[802.1p | dscp | none]* – Specified which incoming packets will be identified for the CoS.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the CoS mapping on the Switch:

```
DES-1210-52/ME:5# config cos mapping port all 802.1p
Command: config cos mapping port all 802.1p



Success.

DES-1210-52/ME:5#
```

show cos mapping

Purpose	To display the information regarding CoS mapping enabled ports and their mapping method.
Syntax	**show cos mapping {port <portlist>}**
Description	The **show cos mapping** command displays the information regarding CoS mapping enabled ports and their mapping method.
Parameters	*<portlist>* - A port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the CoS mapping on the Switch:

```
DES-1210-52/ME:5# show cos mapping port 1-3
Command: show cos mapping port 1-3



Port   Ethernet_Priority    IP_Priority
--------------------------------------------------
```

```
1          802.1p              DSCP
2          802.1p              DSCP
3          802.1p              DSCP

DES-1210-52/ME:5#
```

config cos protocol_mapping

Purpose	To configure the CoS protocol mapping method on the Switch.
Syntax	**config cos protocol_mapping protocol <ip_protocol 1-255> class <class_id 0-3>**
Description	The **config cos protocol_mapping** command is used to configure the CoS protocol mapping method on the Switch.
Parameters	<*ip_protocol 1-255*> - Specifies the protocol IP to be mapped. <*class_id 0-3*> - Specifies the number of the Switch’s hardware priority queue.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the CoS mapping on the Switch:

```
DES-1210-52/ME:5# config cos protocol_mapping protocol 10 class 1
Command: config cos protocol_mapping protocol 10 class 1



Success.

DES-1210-52/ME:5#
```

show cos protocol_mapping

Purpose	To display the CoS protocol mapping information between an incoming packet’s 802.1p priority value.
Syntax	**show cos protocol_mapping {protocol <ip_protocol 1-255>}**
Description	The **show cos protocol_mapping** command is used to display the CoS protocol mapping information between an incoming packet’s 802.1p priority value.
Parameters	<*ip_protocol 1-255*> - Specifies the mapped protocol IP to be displayed.
Restrictions	None.

Example usage:

To display the CoS protocol mapping on the Switch:

```
DES-1210-52/ME:5# show cos protocol_mapping
Command: show cos protocol_mapping

IP Protocol              Class
------------------------------------
10                         1
```

```


DES-1210-52/ME:5#
```

delete cos protocol_mapping

Purpose	To delete the CoS protocol mapping between an incoming packet’s 802.1p priority value.
Syntax	**delete cos protocol_mapping protocol <ip_protocol 1-255>**
Description	The **delete cos protocol_mapping** command is used to delete the CoS protocol mapping between an incoming packet’s 802.1p priority value.
Parameters	*<ip_protocol 1-255>* - Specifies the mapped protocol IP to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the CoS protocol mapping on the Switch:

```
DES-1210-52/ME:5# delete cos protocol_mapping protocol 10
Command: delete cos protocol_mapping protocol 10


Success.

DES-1210-52/ME:5#
```

config cos vlanid_mapping

Purpose	To configure the CoS VLAN id mapping method on the Switch.
Syntax	**config cos vlanid_mapping vid <vlanid 1-4094> class <class_id 0-3>**
Description	The **config cos vlanid_mapping** command is used to configure the CoS VLAN id mapping method on the Switch.
Parameters	*<vlanid 1-4094>* - Specifies the vlan id to be mapped. *<class_id 0-3>* - Specifies the number of the Switch’s hardware priority queue.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure a CoS VLAN id mapping on the Switch:

```
DES-1210-52/ME:5# config cos vlanid_mapping vid 100 class 2
Command: config cos vlanid_mapping vid 100 class 2


Success.

DES-1210-52/ME:5#
```

show cos vlanid_mapping

Purpose	To display the CoS VLAN id mapping information between an incoming packet's 802.1p priority value.
Syntax	**show cos vlanid_mapping {vid <vlanid 1-4094>}**
Description	The **show cos vlanid_mapping** command is used to display the CoS VLAN id mapping information between an incoming packet's 802.1p priority value.
Parameters	*<vlanid 1-4094>* - Specifies the mapped vlan id information to be displayed.
Restrictions	None.

Example usage:

To display the CoS VLAN id mapping on the Switch:

```
DES-1210-52/ME:5# show cos vlanid_mapping
Command: show cos vlanid_mapping

VLAN ID              Class
---------------------------------------
100                    2



DES-1210-52/ME:5#
```

delete cos vlanid_mapping

Purpose	To delete the mapping between an incoming packet's 802.1p priority value.
Syntax	**delete cos vlanid_mapping vid <vlanid 1-4094>**
Description	The **delete cos vlanid_mapping** command is used to delete the mapping between an incoming packet's 802.1p priority value.
Parameters	*<vlanid 1-4094>* - Specifies the mapped vlan id information to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To deleted the CoS VLAN id mapping on the Switch:

```
DES-1210-52/ME:5# delete cos vlanid_mapping vid 100
Command: delete cos vlanid_mapping vid 100



Success.

DES-1210-52/ME:5#
```

config cos tos value

Purpose	To configure the CoS tos on the Switch.

Syntax	**config cos tos value <value 0-7> class <priority 0-7>**
Description	The **config cos tos value** command is used to configure the CoS tos on the Switch.
Parameters	*<value 0-7>* - Specifies the value of the Switch's tos queue. *<priority 0-7>* - Specifies the number of the Switch's hardware priority queue.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure a CoS tos on the Switch:

```
DES-1210-52/ME:5# config cos tos value 1 class 1
Command: config cos tos value 1 class 1



Success.

DES-1210-52/ME:5#
```

show cos tos

Purpose	To display the CoS tos mapping information between an incoming packet's 802.1p priority value.
Syntax	**show cos tos {value <value 0-7>}**
Description	The **show cos tos** command is used to display the CoS tos mapping information.
Parameters	*<value 0-7>* - Specifies the value of the Switch's tos queue.
Restrictions	None.

Example usage:

To display the CoS tos mapping on the Switch:

```
DES-1210-52/ME:5# show cos tos
Command: show cos tos



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

DES-1210-52/ME:5#
```

config cos tcp_port_mapping

Purpose	To configure the CoS TCP port mapping on the Switch.
Syntax	**config cos tcp_port_mapping destination_port <value 0-65535> class <class_id 0-3>**
Description	The **config cos tcp_port_mapping** command is used to configure the CoS TCP port mapping on the Switch.
Parameters	*<value 0-65535>* - Specifies the tcp port number to be mapped. *<class_id 0-3>* - Specifies the number of the Switch's hardware priority queue.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the CoS TCP port mapping on the Switch:

```
DES-1210-52/ME:5# config cos tcp_port_mapping destination_port 500
class 1
Command: config cos tcp_port_mapping destination_port 500 class 1



Success.

DES-1210-52/ME:5#
```

show cos tcp_port_mapping

Purpose	To displays the CoS TCP port mapping information on the Switch.
Syntax	**show cos tcp_port_mapping {destination_port <value 0-65535>}**
Description	The **show cos tcp_port_mapping** command is used to display the CoS TCP port mapping information on the Switch.
Parameters	*<value 0-65535>* - Specifies the mapped tcp port information to be displayed.
Restrictions	None.

Example usage:

To display the CoS TCP port mapping on the Switch:

```
DES-1210-52/ME:5# show cos tcp_port_mapping
Command: show cos tcp_port_mapping

TCP Port          Class
-----------------------------------
500                 1


DES-1210-52/ME:5#
```

delete cos tcp_port_mapping

Purpose	To delete the CoS TCP port mapping information on the Switch.
Syntax	**delete cos tcp_port_mapping destination_port <value 0-65535>**

Description	The **delete cos tcp_port_mapping** command is used to delete the CoS TCP port mapping information on the Switch.
Parameters	<*value 0-65535*> - Specifies the mapped tcp port information to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the CoS TCP port mapping on the Switch:

```
DES-1210-52/ME:5# delete cos tcp_port_mapping destination_port 500
Command: delete cos tcp_port_mapping destination_port 500



Success.

DES-1210-52/ME:5#
```

config cos udp_port_mapping

Purpose	To configure the CoS UDP port mapping on the Switch.
Syntax	**config cos udp_port_mapping destination_port <value 0-65535> class <class_id 0-3>**
Description	The **config cos udp _port_mapping** command is used to configure the CoS UDP port mapping on the Switch.
Parameters	<*value 0-65535*> - Specifies the udp port number to be mapped. <*class_id 0-3*> - Specifies the number of the Switch's hardware priority queue.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the CoS UDP port mapping on the Switch:

```
DES-1210-52/ME:5# config cos udp_port_mapping destination_port 500
class 2
Command: config cos udp_port_mapping destination_port 500 class 2



Success.

DES-1210-52/ME:5#
```

show cos udp _port_mapping

Purpose	To displays the CoS UDP port mapping information on the Switch.
Syntax	**show cos udp_port_mapping {destination_port <value 0-65535>}**
Description	The **show cos udp _port_mapping** command is used to display the CoS UDP port mapping information on the Switch.
Parameters	<*value 0-65535*> - Specifies the mapped udp port information to be displayed.

Restrictions	None.

Example usage:

To display the CoS UDP port mapping on the Switch:

```
DES-1210-52/ME:5# show cos udp_port_mapping
Command: show cos udp_port_mapping

UDP Port              Class
-----------------------------------------
500                   2



DES-1210-52/ME:5#
```

delete cos udp_port_mapping

Purpose	To delete the CoS UDP port mapping information on the Switch.
Syntax	**delete cos udp_port_mapping destination_port <value 0-65535>**
Description	The **delete udp tcp_port_mapping** command is used to delete the CoS TCP port mapping information on the Switch.
Parameters	<*value 0-65535*> - Specifies the mapped udp port information to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the CoS UDP port mapping on the Switch:

```
DES-1210-52/ME:5# delete cos udp_port_mapping destination_port 500
Command: delete cos udp_port_mapping destination_port 500



Success.

DES-1210-52/ME:5#
```

config 802.1p user_priority

Purpose	To map the 802.1p user priority of an incoming packet to one of the four hardware classes of service available on the Switch.
Syntax	**config 802.1p user_priority <priority 0-7> <class_id 0-7>**
Description	The **config 802.1p user_priority** command configures the way the Switch maps an incoming packet, based on its 802.1p user priority tag, to one of the four hardware priority classes of service available on the Switch. The Switch's default is to map the incoming 802.1p priority values to the four hardware classes of service according to the following chart: 802.1p value Switch Priority Queue Switch Priority Queue(stack) ----------------- ---------------------------- ------------------------------------ 0 1 0

	1	0	0
	2	0	0
	3	1	0
	4	2	1
	5	2	1
	6	3	2
	7	3	2
Parameters	<*priority 0-7*> − The 802.1p priority value (0 to 7) to map to one of the Switch's four hardware priority classes of service. <*class_id 0-7*> − The Switch's hardware priority class of service (0 to 3) to map to the 802.1p priority value specified above.		
Restrictions	Only administrator or operator level users can issue this command.		

Example usage:

To configure 802.1 user priority on the Switch:

```
DES-1210-52/ME:5# config 802.1p user_priority 2 0
Command: config 802.1p user_priority 2 0

Success.

DES-1210-52/ME:5#
```

show 802.1p user_priority

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

Example usage:

To show 802.1p user priority:

```
DES-1210-52/ME:5# show 802.1p user_priority
Command: show 802.1p user_priority


QOS Class of Traffic

Priority-0  ->  <Class-2>
Priority-1  ->  <Class-0>
Priority-2  ->  <Class-1>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-4>
Priority-5  ->  <Class-5>
```

```
Priority-6  ->  <Class-6>
Priority-7  ->  <Class-7>

DES-1210-52/ME:5#
```

config 802.1p default_priority

Purpose	To assign an 802.1p priority tag to an incoming untagged packet that has no 802.1p priority tag.
Syntax	**config 802.1p default_priority [<portlist> | all] <priority 0-7>**
Description	The **config 802.1p default_priority** command specifies the 802.1p priority value an untagged, incoming packet is assigned before being forwarded to its destination.
Parameters	*<portlist>* − A port or range of ports to be configured. *all* − Specifies that the config 802.1p default_priority command applies to all ports on the Switch. *<priority 0-7>* − The 802.1p priority value that an untagged, incoming packet is granted before being forwarded to its destination.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure 802.1p default priority on the Switch:

```
DES-1210-52/ME:5# config 802.1p default_priority all 4
Command: config 802.1p default_priority all 4

Success.

DES-1210-52/ME:5#
```

show 802.1p default_priority

Purpose	To display the currently configured 802.1p priority value that is assigned to an incoming, untagged packet before being forwarded to its destination.
Syntax	**show 802.1p default_priority {<portlist>}**
Description	The **show 802.1p default_priority** command displays the currently configured 802.1p priority value that is assigned to an incoming, untagged packet before being forwarded to its destination.
Parameters	*<portlist>* − A port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the current port 1-4 802.1p default priority configuration on the Switch:

```
DES-1210-52/ME:5# show 802.1p default_priority 1-4
Command: show 802.1p default_priority 1-4

Port  Default Priority  Effective Priority
----  ----------------------  --------------------------
1          4                  4
```

```
2         4              4
3         4              4
4         4              4

DES-1210-52/ME:5#
```

config scheduling_mechanism

Purpose	To configure the scheduling mechanism for the QoS function.
Syntax	**config scheduling_mechanism [strict | wrr]**
Description	The **config scheduling_mechanism** command configures the scheduling mechanism for the QoS function. It allows the user to select between a round robin (WRR) and a strict mechanism for emptying the priority classes of service of the QoS function. The Switch contains four hardware priority classes of service. Incoming packets must be mapped to one of these four hardware priority classes of service, or queues. This command is used to specify the rotation by which these four hardware priority queues are emptied. The Switch's default is to empty the four hardware priority queues in order − from the highest priority hardware queue (class 3) to the lowest priority hardware queue (class 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. A lower priority hardware queue will be pre-empted from emptying its queue if a packet is received on a higher priority hardware queue. The packet received on the higher priority hardware queue transmits its packet before allowing the lower priority hardware queue to resume clearing its queue.
Parameters	*strict* – Specifies that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin. *wrr* – Specifies that the priority classes of service are to empty packets in a weighted roundrobin (WRR) order.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DES-1210-52/ME:5# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DES-1210-52/ME:5#
```

show scheduling_mechanism

Purpose	To display the current traffic scheduling mechanisms in use on the Switch.
Syntax	**show scheduling_mechanism**
Description	The **show scheduling_mechanism** command displays the current traffic scheduling mechanisms in use on the Switch.

Parameters	None.
Restrictions	None.

Example usage:

To show the scheduling mechanism:

```
DES-1210-52/ME:5# show scheduling_mechanism
Command: show scheduling_mechanism

QOS Scheduling_mechanism

scheduling_mechanism   :  Strict Priority

DES-1210-52/ME:5#
```

config dscp mode

Purpose	To enable setting the DSCP User Priority
Syntax	**config dscp mode**
Description	The **config dscp mode** command enables the DSCP mode on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To enable the DSCP mode:

```
DES-1210-52/ME:5# config dscp mode
Command: config dscp mode

DSCP mode Success.

Success.

DES-1210-52/ME:5#
```

config dscp_mapping

Purpose	To enable setting the DSCP User Priority
Syntax	**config dscp_mapping dscp_value <value 0-63> class <class_id 0-7>**
Description	The **config dscp_mapping** command enables mapping the DSCP value (the priority) to a specific queue (the class_id).
Parameters	*<value 0-63>* –The selected value of priority. The value may be between 0 and 63. *<class_id 0-7>* – The class_id (queue) mapped to the priority. The value may be between 0 and 3
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the DSCP mapping with value 10 and class 2:

```
DES-1210-52/ME:5# config dscp_mapping dscp_value 10 class 2
Command: config dscp_mapping dscp_value 10 class 2

Success.

DES-1210-52/ME:5#
```

show dscp_mapping

Purpose	To display the setting of DSCP mapping.
Syntax	**show dscp_mapping {dscp_value <value 0-63>}**
Description	The **show dscp_mapping** command displays the mapping of DSCP value.
Parameters	*dscp_value <value 0-63>* - The selected value of priority will be dispalyed. The value may be between 0 and 63.
Restrictions	None.

Example usage:

To display the DSCP mapping with value 10:

```
DES-1210-52/ME:5# show dscp_mapping dscp_value 10
Command: show dscp_mapping dscp_value 10

DSCP    Class
-------------------------
10          2

DES-1210-52/ME:5#
```

26

RMON COMMANDS

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

Command	Parameter
enable rmon	
disable rmon	
create rmon alarm	<alarm_index 1-65535> <OID_variable 255> <interval 1-2147482647> [absolute | delta] rising-threshold <value 0-2147483647> <rising_event_index 1-65535> falling-threshold <value 0-2147483647> <falling_event_index 1-65535> {[owner <owner_string 32>]}
delete rmon alarm	<alarm_index 1-65535>
create rmon collection stats	<stats_index 1-65535> port <ifindex> owner <owner_string 32>
delete rmon collection stats	<stats_index 1-65535>
create rmon collection history	<hist_index 1-65535> port <ifindex> {buckets <buckets_req 1-50> interval <interval 1-3600> owner <owner_string 32>}
delete rmon collection history	<hist_index 1-65535>
create rmon event	<event_index 1-65535> description <desc_string 128> {[log | owner <owner_string 32> | trap <community_string 32>]}
delete rmon event	<event_index 1-65535>
show rmon	
show rmon statistics	{<stats_index 1-65535>}

Each command is listed in detail, as follows:

enable rmon	
Purpose	To enable remote monitoring (RMON) status for the SNMP function.
Syntax	**enable rmon**
Description	The **enable rmon** command enables remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the RMON feature on the Switch:

```
DES-1210-52/ME:5# enable rmon
```

```
Command: enable rmon



Success.
DES-1210-52/ME:5#
```

disable rmon

Purpose	To disable remote monitoring (RMON) status for the SNMP function.
Syntax	**disable rmon**
Description	The **disable rmon** command disables remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the RMON feature on the Switch:

```
DES-1210-52/ME:5# disable rmon
Command: disable rmon



Success.
DES-1210-52/ME:5#
```

create rmon alarm

Purpose	To allow the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.
Syntax	**create rmon alarm <alarm_index 1-65535> <OID_variable 255> <interval 1-2147482647> [absolute | delta] rising-threshold <value 0-2147483647> <rising_event_index 1-65535> falling-threshold <value 0-2147483647> <falling_event_index 1-65535> {[owner <owner_string 32>]}**
Description	The **create rmon alarm** command allows the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.
Parameters	*<alarm_index>* − Specifies the alarm number. *<OID_variable 255>* − Specifies the MIB variable value. *<interval 1-2147482647>* − Specifies the alarm interval time in seconds. *[absolute* | *delta]* − Specifies the sampling method for the selected variable and comparing the value against the thresholds. The possible values are absolute and delta: • *absolute* –Compares the values directly with the thresholds at the end of the sampling interval. • *delta* –Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold. *rising-threshold <value 0-2147483647>* − Specifies the rising

	counter value that triggers the rising threshold alarm. *<rising_event_index 1-65535>* − Specifies the event that triggers the specific alarm. *falling-threshold <value 0-2147483647>* − Specifies the falling counter value that triggers the falling threshold alarm. *<falling_event_index 1-65535>* − Specifies the event that triggers the specific alarm. The possible field values are user defined RMON events. *owner <owner_string 32>* − Specifies the device or user that defined the alarm.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON alarm on the Switch:

```
DES-1210-52/ME:5# create rmon alarm 20 1 100 absolute rising-threshold
200 2 falling-threshold 100 1 owner dlink
Command: create rmon alarm 20 1 100 absolute rising-threshold 200 2
falling-threshold 100 1 owner dlink



Success.
DES-1210-52/ME:5#
```

delete rmon alarm

Purpose	To remove the network alarms.
Syntax	**delete rmon alarm <alarm_index 1-65535>**
Description	The **delete rmon alarm** command removes the network alarms.
Parameters	*<alarm_index 1-65535>* − Specifies the alarm number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON alarm on the Switch:

```
DES-1210-52/ME:5# delete rmon alarm 100
Command: delete rmon alarm 100

Success.
DES-1210-52/ME:5#
```

create rmon collection stats

Purpose	To allow user to configure the rmon stats settings on the Switch.
Syntax	**create rmon collection stats <stats_index 1-65535> port <ifindex> owner <owner_string 32>**
Description	The **create rmon collection stats** command allows user to configure the rmon stats settings on the Switch.
Parameters	*<stats_index 1-65535>* − Specifies the stats number.

	port <ifindex> − Specifies the port from which the RMON information was taken. *owner <owner_string 32>* − Specifies the device or user that defined the stats.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection stats on the Switch:

```
DES-1210-52/ME:5# create rmon collection stats 100 port 1 owner dlink
Command: create rmon collection stats 100 port 1 owner dlink



Success.
DES-1210-52/ME:5#
```

delete rmon collection stats

Purpose	To remove the network collection stats.
Syntax	**delete rmon collection stats <stats_index 1-65535>**
Description	The **delete rmon collection stats** command removes the network collection stats on the Switch.
Parameters	*<stats_index 1-65535>* − Specifies the stats number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON collection stats on the Switch:

```
DES-1210-52/ME:5# delete rmon collection stats 100
Command: delete rmon collection stats 100

Success.
DES-1210-52/ME:5#
```

create rmon collection history

Purpose	To allow user to configure the rmon history settings on the Switch.
Syntax	**create rmon collection history <hist_index 1-65535> port <ifindex> {buckets <buckets_req 1-50> interval <interval 1-3600> owner <owner_string 32>}**
Description	The **create rmon collection history** command allows user to configure the rmon history settings on the Switch.
Parameters	*<hist_index 1-65535>* − Indicates the history control entry number. *port <ifindex>* − Specifies the port from which the RMON information was taken. *buckets <buckets_req 1-50>* − Specifies the number of buckets that the device saves. *interval <interval 1-3600>* − Specifies in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes).

	owner <owner_string 32> − Specifies the RMON station or user that requested the RMON information.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection history on the Switch:

```
DES-1210-52/ME:5# create rmon collection history 120 port 2 buckets 25
Command: create rmon collection history 120 port 2 buckets 25



Success.
DES-1210-52/ME:5#
```

delete rmon collection history

Purpose	To remove the network collection history.
Syntax	**delete rmon collection history <hist_index 1-65535>**
Description	The **delete rmon collection history** command removes the network collection history on the Switch.
Parameters	*<hist_index 1-65535>* − Specifies the alarm history number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON collection history on the Switch:

```
DES-1210-52/ME:5# delete rmon collection history 2
Command: delete rmon collection history 2

Success.
DES-1210-52/ME:5#
```

create rmon event

Purpose	To provide user to configure the settings of rmon event on the Switch.
Syntax	**create rmon event <event_index 1-65535> description <desc_string 128> {[log | owner <owner_string 32> | trap <community_string 32>]}**
Description	The **create rmon event** command allows user to provides user to configure the settings of rmon event on the Switch.
Parameters	*<event_index 1-65535>* − Specifies the event number. *description <desc_string 128>* − Specifies the user-defined event description. *log* − Indicates that the event is a log entry. *owner <owner_string* 32> − Specifies the time that the event occurred. *trap <community_string* 32> − Specifies the community to which the event belongs.

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

Example usage:

To create a RMON collection history on the Switch:

```
DES-1210-52/ME:5# create rmon event 125 description linkrmon owner
dlink
Command: create rmon event 125 description linkrmon owner dlink



Success.
DES-1210-52/ME:5#
```

delete rmon event

Purpose	To remove the network event.
Syntax	**delete rmon event <event_index 1-65535>**
Description	The **delete rmon event** command removes the network event on the Switch.
Parameters	*<event_index 1-65535>* − Specifies the event number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON event on the Switch:

```
DES-1210-52/ME:5# delete rmon event 2
Command: delete rmon event 2

Success.
DES-1210-52/ME:5#
```

show rmon

Purpose	To display remote monitoring (RMON) status for the SNMP function.
Syntax	**show rmon {alarms | events | history | statistics}**
Description	The **show rmon** command displays remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	*{alarms* | *events* | *history* | *statistics}* – Specify to show the specified information.
Restrictions	None.

Example usage:

To display the RMON feature on the Switch:

```
DES-1210-52/ME:5# show rmon alarms events
Command: show rmon alarms events



RMON is enabled
```

```
Alarm table is empty
Event table is empty

Success.
DES-1210-52/ME:5#
```

show rmon statistics

Purpose	To display remote monitoring (RMON) statistics for the SNMP function.
Syntax	**show rmon statistics {<stats_index 1-65535>}**
Description	The **show rmon** command displays remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	*<stats_index 1-65535>* − Specifies the statistics index of RMON to be displayed.
Restrictions	None.

Example usage:

To display the RMON statistics on the Switch:

```
DES-1210-52/ME:5# show rmon statistics
Command: show rmon statistics



RMON is enabled
Ethernet Statistics table is empty

Success.
DES-1210-52/ME:5#
```

27

PORT MIRRORING COMMANDS

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

Command	Parameter
enable mirror	
disable mirror	
config mirror target	<short 1-52> [add | delete] source ports <portlist> [both | rx | tx]
delete mirror	target <port> source <port>
show mirror	

Each command is listed in detail, as follows:

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

Example usage:

To enable the mirroring feature:

```
DES-1210-52/ME:5# enable mirror
Command: enable mirror

Success.

DES-1210-52/ME:5#
```

disable mirror	
Purpose	Used to disable a previously entered port mirroring configuration.
Syntax	**disable mirror**
Description	The **disable mirror** command, combined with the enable mirror command above, allows the user to enter a port mirroring configuration into the Switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.

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

Example usage:

To disable mirroring configurations:

```
DES-1210-52/ME:5# disable mirror
Command: disable mirror

Success.

DES-1210-52/ME:5#
```

config mirror target

Purpose	To configure a mirror port − source port pair on the Switch.
Syntax	**config mirror target <short 1-52> [add | delete] source ports <portlist> [both | rx | tx]**
Description	The **config mirror target** command allows a port to have all of its traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, one can specify that only traffic received by or sent by one or both is mirrored to the target port.
Parameters	*target <short 1-52>* − Specifies the port that mirrors traffic forwarding. *[add | delete]* − Specifies to add or delete the target port. *source ports <portlist>* – Specifies the port or ports being mirrored. This cannot include the target port. *rx* – Allows mirroring of packets received by (flowing into) the source port. *tx* – Allows mirroring of packets sent to (flowing out of) the source port. *both* – Allows mirroring of all the packets received or sent by the source port. *Comment*: The user can define up to 8 source ports and one destination port. One source port can be configured each time using one CLI command, So in order to configure multiple source ports, multiple CLI commands should be used.
Restrictions	A target port cannot be listed as a source port. Only Administrator or operator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DES-1210-52/ME:5# config mirror target 2 add source ports 8-10 both
Command: config mirror target 2 add source ports 8-10 both




Success.

DES-1210-52/ME:5#
```

show mirror

Purpose	To show the current port mirroring configuration on the Switch.
Syntax	**show mirror**
Description	The **show mirror** command displays the current port mirroring configuration on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display mirroring configuration:

```
DES-1210-52/ME:5# show mirror
Command: show mirror


Port Mirror  is enabled
Target Port : 2
Source Port : 8
Direction   : Both

Target Port : 2
Source Port : 9
Direction   : Both

Target Port : 2
Source Port : 10
Direction   : Both


DES-1210-52/ME:5#
```

28

VLAN COMMANDS

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

Command	Parameter
create vlan	<string 32> tag <int 2-4094> type_1q_vlan_advertisement
delete vlan	[<vlan_name 32> | vlanid <vidlist >]
config vlan	[<vlan_name 32> | vlanid <vlanid 1-4094>] [[add [tagged | untagged | forbidden] | delete] [<portlist> | name <vlan_name 32>] {advertisement [enable | disable]}
config gvrp	[state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [Tagged_Only | All_Frames] | pvid <vlanid 1-4094>]
config gvrp timer	[join_timer <sec 100-100000> | leave_timer <sec 100-100000> | leave-all_timer <sec 100-100000>]
enable gvrp	
disable gvrp	
show vlan	{<vlan_name 32> | vlanid <vidlist> | ports <portlist>}
create dot1v_protocol_group group_id <id 1-16>	{group_name <name 32>}
config dot1v_protocol_group	[group_id <id 1-16> | group_name <name 32>] [add | delete] protocol [ethernet_2 <hex 0x0-0xffff> | ieee802.3_snap <hex 0x0-0xffff>]
delete dot1v_protocol_group	[group_id <id 1-16> | group_name <name 32> | all]
show dot1v_protocol_group	{group_id <id 1-16> | group_name <name 32>}
config port dot1v ports all	[add | delete] protocol_group [group_name <name 32> | group_id <id 1-16>] [vlan <vlan_name 32> | vlanid <id 1-4094>]
show port dot1v	{ports <portlist>}
show gvrp	{<portlist>}
show gvrp timer	
enable vlan_trunk	
disable vlan_trunk	
show vlan_trunk	
config vlan_trunk ports	[<portlist> | all] state [enable | disable]
enable asymmetric_ vlan	
disable asymmetric_vlan	

Command	Parameter
show asymmetric_vlan	
enable pvid auto_assign	
disable pvid auto_assign	
show pvid auto_assign	

Each command is listed in detail, as follows:

create vlan

Purpose	To create a VLAN on the Switch.
Syntax	**create vlan <string 32> tag <int 2-4094> type_1q_vlan_advertisement**
Description	The **create vlan** command creates a VLAN on the Switch.
Parameters	*<string 32>* − The name of the VLAN to be created. *tag <int 2-4094>* − The VLAN ID of the VLAN to be created. The allowed values range from 2 to 4094. *type_1q_vlan_advertisement* − Specifies the 1q vlan advertisement on the Switch.
Restrictions	Each VLAN name can be up to 32 characters. If the VLAN is not given a tag, it will be a port-based VLAN. Only administrator or operator-level users can issue this command.

Example usage:

To create a VLAN rd2, tag 3:

```
DES-1210-52/ME:5# create vlan rd2 tag 3 type_1q_vlan_advertisement
Command: create vlan rd2 tag 3 type_1q_vlan_advertisement



Success.
DES-1210-52/ME:5#
```

delete vlan

Purpose	To delete a previously configured VLAN on the Switch.
Syntax	**delete vlan [<vlan_name 32> | vlanid <vidlist>]**
Description	The **delete vlan** command deletes a previously configured VLAN on the Switch.
Parameters	*<vlan_name 32>* − The name of the VLAN to be deleted. *vlanid <vidlist>* − The VLAN of the VLAN to be deleted. The range is between 2-4092.
Restrictions	Only administrator or operator-level users can issue this command. A user is required to disable Guest VLAN before deleting a VLAN.

Example usage:

To remove a vlan which VLAN ID is 2:

```
DES-1210-52/ME:5# delete vlan vlanid 2
Command: delete vlan vlanid 2

Success.
DES-1210-52/ME:5#
```

config vlan

Purpose	To add additional ports to a previously configured VLAN and to modify a VLAN name.
Syntax	**config vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] [[add [tagged | untagged | forbidden] | delete] [<portlist> | name <vlan_name 32>] {advertisement [enable | disable]}**
Description	The **config vlan** command allows the user to add or delete ports to the port list of a previously configured VLAN. You can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagged.
Parameters	*<vlan_name 32>* − The name of the VLAN to be configure. *vlanid <vidlist>* − The ID of the VLAN to which to add ports. *add* − Specifies that ports are to be added to a previously created vlan. *delete* - Specifies that ports are to be deleted from a previously created vlan. *tagged* − Specifies the additional ports as tagged. *untagged* − Specifies the additional ports as untagged. *forbidden* − Specifies the additional ports as forbidden. *<portlist>* − A port or range of ports to be added to or deleted from the VLAN. *name <vlan_name 32>* − Enter the vlan name for the specified vlan id. *advertisement [enable | disable]* − Specifies that the vlan advertisement is enabled or disabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To add ports 4 through 8 as tagged ports to the VLAN 3:

```
DES-1210-52/ME:5# config vlan vlanid 3 add tagged 4-8
Command: config vlan vlanid 3 add tagged 4-8

Success.
DES-1210-52/ME:5#
```

config gvrp

Purpose	To configure configures the Group VLAN Registration Protocol on the Switch. The user can configure ingress checking and acceptable frame tagged only, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).
Syntax	**config gvrp [<portlist> | all] [state [enable | disable] |**

	ingress_checking [enable | disable] | acceptable_frame [Tagged_Only | All_Frames] | pvid <vlanid 1-4094>]
Description	The **config gvrp** command configures the Group VLAN Registration Protocol on the Switch. The user can configure ingress checking and acceptable frame tagged only, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).
Parameters	*<portlist>* − A port or range of ports for which to configure GVRP. *all* − configure GVRP on ports. *state [enable* | *disable]* - enable and disable GVRP *ingress_checking [enable* | *disable]* − Enables or disables ingress checking for the specified port list. *acceptable_frame [tagged_only* | *admit_all]* – Defines the type of frame accepted. Acceptable frames can be limited to tagged frames only (*tagged_only*) or can accept tagged and untagged (*admit_all*). *pvid <vlanid 1-4094>* – Specifies the default VLAN associated with the port, by VLAN ID.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To set the ingress checking status:

```
DES-1210-52/ME:5# config gvrp all ingress_checking enable
Command: config gvrp all ingress_checking enable

Success.

DES-1210-52/ME:5#
```

config gvrp timer

Purpose	To configure GVRP timer on the Switch.
Syntax	**config gvrp timer [join_timer <sec 100-100000> | leave_timer <sec 100-100000> | leave-all_timer <sec 100-100000>]**
Description	The **config gvrp timer** command configures the Group VLAN Registration Protocol on the Switch. The user can configure ingress checking and acceptable frame tagged only, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).
Parameters	*join_timer <sec 100-100000>* − Specifies the join time for the GVRP on the Switch. The time range is from 100 to 100000 seconds. *leave_timer <sec 100-100000>* − Specifies the leave time for the GVRP on the Switch. The time range is from 100 to 100000 seconds. *leave-all_timer_<sec 100-100000>* − Specifies the leave all time for the GVRP on the Switch. The time range is from 100 to 100000 seconds.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To set the GVRP packet join time:

```
DES-1210-52/ME:5# config gvrp timer join_timer 100
Command: config gvrp timer join_timer 100

```

```
Success.

DES-1210-52/ME:5#
```

enable gvrp

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

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DES-1210-52/ME:5# enable gvrp
Command: enable gvrp

Success.
DES-1210-52/ME:5#
```

disable gvrp

Purpose	To disable GVRP on the Switch.
Syntax	**disable gvrp**
Description	The **disable gvrp** command, along with the **enable gvrp** command above, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the ports and the LAGs.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DES-1210-52/ME:5# disable gvrp
Command: disable gvrp

Success.
DES-1210-52/ME:5#
```

show vlan

Purpose	To display the current VLAN configuration on the Switch
Syntax	**show vlan {<vlan_name 32> | vlanid <vidlist> | ports <portlist>}**
Description	The **show vlan** 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>* - Specify the VLAN name to be displayed. *vlanid <vidlist>* − Specify the VLAN id to be displayed. *ports <portlist>* − Specify the ports to be displayed.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DES-1210-52/ME:5# show vlan
Command: show vlan

VID                    : 1       VLAN NAME     : default
VLAN Type              : Static
VLAN Advertisement : Disabled
Member Ports           : 1-52
Untagged Ports         : 1-52
Forbidden Ports        :

VID                    : 3       VLAN NAME     : rd2
VLAN Type              : Static
VLAN Advertisement : Disabled
Member Ports           :
Untagged Ports          :
Forbidden Ports         :

DES-1210-52/ME:5#
```

create dot1v_protocol_group

Purpose	To create a protocol group for protocol VLAN function.
Syntax	**create dot1v_protocol_group group_id <id 1-16> {group_name <name 32>}**
Description	The **create dot1v_protocol_group** command creates a protocol group for protocol VLAN function.
Parameters	group_id <id 1-16> − The ID of a protocol group which is used to identify a set of protocols. *group_name <name 32>* − The name of the protocol group. The maximum length is 32 characters.
Restrictions	Only Administrator and Operator and Power-User-level users can issue this command.

Example usage:

To create a protocol group:

```
DES-1210-52/ME:5# create dot1v_protocol_group group_id 1 group_name
group1
Command: create dot1v_protocol_group group_id 1 group_name group1



Success.
DES-1210-52/ME:5#
```

config dot1v_protocol_group

Purpose	To add/delete a protocol to/from a protocol group.
Syntax	**config dot1v_protocol_group [group_id <id 1-16> | group_name <name 32>] [add | delete] protocol [ethernet_2 <hex 0x0-0xffff> | ieee802.3_snap <hex 0x0-0xffff>]**
Description	The **config dot1v_protocol_group** command adds/deletes a protocol to/from a protocol group.The selection of a protocol can be a pre-defined protocol type or a user specified protocol type.
Parameters	group_id <id 1-16> − The ID of protocol group which is used to identify a set of protocols. *group_name* <*name 32*> − The name of the protocol group. The maximum length is 32 chars. <*hex 0x0-0xffff*> − The protoocl vlaue 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.
Restrictions	Only Administrator and Operator and Power-User-level users can issue this command.

Example usage:

To add a protocol IPv6 to protocol group 2:

```
DES-1210-52/ME:5# config dot1v_protocol_group group_id 2 add protocol
ethernet_2 0x86DD
Command: config dot1v_protocol_group group_id 2 add protocol ethernet_2
0x86DD



 The protocol value configured to add will take effect on both frame types
ethernet_2 and ieee802.3_snap.



Success.

DES-1210-52/ME:5#
```

delete dot1v_protocol_group

Purpose	To delete a protocol group.
Syntax	**delete dot1v_protocol_group [group_id <id 1-16> | group_name <name 32> | all]**
Description	The **delete dot1v_protocol_group** command deletes a protocol group.
Parameters	group_id <id 1-16> − Specifies the group ID to be deleted. *group_name* <*name 32*> − The name of the protocol group. The maximum length is 32 characters.
Restrictions	Only Administrator and Operator and Power-User-level users can issue this command.

Example usage:

To delete a protocol group 1:

```
DES-1210-52/ME:5# delete dot1v_protocol_group all
Command: delete dot1v_protocol_group all


Success.
DES-1210-52/ME:5#
```

show dot1v_protocol_group

Purpose	To display the protocols defined in a protocol group.
Syntax	**show dot1v_protocol_group {group_id <id 1-16> | group_name <name 32>}**
Description	The **show dot1v_protocol_group** command displays the protocols defined in protocol groups.
Parameters	group_id <id 1-16> − Specifies the group ID to be displayed. *group_name <name 32>* − The name of the protocol group. The maximum length is 32 characters.
Restrictions	None.

Example usage:

To display the protocol group ID 2:

```
DES-1210-52/ME:5# show dot1v_protocol_group group_id 2
Command: show dot1v_protocol_group group_id 2


Group ID   Protocol Group Name      Frame Type      Protocol Value
--------- ---------------------- -------------   ---------------
2          group1                  EthernetII      86dd
2          group1                  IEEE802.3 SNAP  86dd


Total Entries: 1


DES-1210-52/ME:5#
```

config port dot1v ports all

Purpose	To assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured.
Syntax	**config port dot1v ports all [add | delete] protocol_group [group_name <name 32> | group_id <id 1-16>] [vlan <vlan_name 32> | vlanid <id 1-4094>]**
Description	The **config port dot1v ports all** command assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured.
Parameters	*[add | delete]* − *group_name <name 32>* − The name of the protocol group. The maximum length is 32 chars.

	group_id <id 1-16> − The ID of protocol group which is used to identify a set of protocols. *<vlan_name 32>* − Specify the VLAN name to be configured. *<id 1-4094>* − Specify the VLAN id to be configured.
Restrictions	Only Administrator and Operator and Power-User-level users can issue this command.

Example usage:

To configure the group ID 4 to be associated with VLAN 2:

```
DES-1210-52/ME:5# config port dot1v ports all add protocol_group group_id
4 vlan vlan2
Command: config port dot1v ports all add protocol_group group_id 4 vlan
vlan2



Success.

DES-1210-52/ME:5#
```

show port dot1v

Purpose	To display the VLAN to be associated with untagged packets ingressed from a port based on the protocol group.
Syntax	**show port dot1v {ports <portlist>}**
Description	The **show port dot1v** command is used to display the VLAN to be associated with untagged packets ingressed from a port based on the protocol group.
Parameters	*ports <portlist>* − Specify a range of ports to be displayed. If not specified, information for all ports will be displayed.
Restrictions	None.

Example usage:

To display the protocol VLAN information for ports 1 to 2:

```
DES-1210-52/ME:5# show port dot1v ports 1-2
Command: show port dot1v ports 1-2


Port: 1
No valid dot1v entry!

Port: 2
No valid dot1v entry!

Total Entries: 0


DES-1210-52/ME:5#
```

show gvrp

Purpose	To display the GVRP status for a port list or port channel on the Switch.
Syntax	**show gvrp {<portlist>}**
Description	The **show gvrp** command displays the GVRP status for a port list or a port channel 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 5~8 status:

```
DES-1210-52/ME:5# show gvrp 5-8
Command: show gvrp 5-8

Global GVRP  : Enable

Port   PVID   GVRP State   Ingress Checking   Acceptable Frame Type
----   ----   ----------   ----------------   ---------------------
5      1      Enable       Enable             All Frames
6      1      Enable       Enable             All Frames
7      1      Enable       Enable             All Frames
8      1      Enable       Enable             All Frames

Total Entries  : 4

DES-1210-52/ME:5#
```

show gvrp timer

Purpose	To display the GVRP timer information on the Switch.
Syntax	**show gvrp timer**
Description	The **show gvrp** command displays the GVRP timer on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display GVRP timer information:

```
DES-1210-52/ME:5# show gvrp timer
Command: show gvrp timer


Garp Timer Info (in milli seconds)
-------------------------------------


Join-time    Leave-time    Leave-all-time
----------   ----------    --------------
```

```
100         600           10000

DES-1210-52/ME:5#
```

enable vlan_trunk

Purpose	To enable VLAN trunking on the switch.
Syntax	**enable vlan_trunk**
Description	The **enable vlan_trunk** command, along with the **disable vlan_trunk** command below, is used to enable and disable VLAN trunking on the Switch, without changing the VLAN trunking configuration on the ports.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable vlan_trunk on the switch:

```
DES-1210-52/ME:5#enable vlan_trunk
Command: enable vlan_trunk

Success.
DES-1210-52/ME:5#
```

disable vlan_trunk

Purpose	To disable VLAN Trunking on the switch.
Syntax	**disable vlan_trunk**
Description	The **disable vlan_trunk** command, along with the **enable vlan_trunk** command below, is used to disable and enable VLAN Trunking on the Switch, without changing the VLAN Trunking configuration on the ports.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable vlan_trunk on the switch:

```
DES-1210-52/ME:5# disable vlan_trunk
Command: disable vlan_trunk

Success.
DES-1210-52/ME:5#
```

show vlan_trunk

Purpose	To display the current VLAN Trunking configuration on the Switch.
Syntax	**show vlan_trunk**
Description	The **show vlan_trunk** command displays summary information about VLAN trunking status and configured ports.

Parameters	None.
Restrictions	None.

Example usage:

To display the Switch's current VLAN_trunk settings:

```
DES-1210-52/ME:5# show vlan_trunk
Command: show vlan_trunk


VLAN Trunk Status      :Enable
Member Ports           :None

DES-1210-52/ME:5#
```

config vlan_trunk ports

Purpose	To configure VLAN Trunking port settings on the Switch.
Syntax	**config vlan_trunk ports [<portlist> | all] state [enable | disable]**
Description	The **config vlan_trunk ports** command configures the VLAN trunking port settings on the Switch. The user can enable VLAN Trunking and define ports to be added to the VLAN Trunking settings.
Parameters	*[<portlist>* | *all]* − A port, range of ports or all ports for which to configure VLAN Trunking. *state [enable* | *disable]* − enable and disable VLAN trunking.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To define VLAN Trunking:

```
DES-1210-52/ME:5# config vlan_trunk ports all state enable
Command: config vlan_trunk ports all state enable

Success.
DES-1210-52/ME:5#
```

enable asymmetric_vlan

Purpose	To enable Asymmetric VLAN on the switch.
Syntax	**enable asymmetric_vlan**
Description	The **enable asymmetric_vlan** command, along with the **disable enable asymmetric_vlan** command below, is used to enable and disable Asymmetric VLAN on the Switch
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable Asymettric VLAN on the switch:

```
DES-1210-52/ME:5# enable asymmetric_vlan
```

```
Command: enable asymmetric_vlan

Warning: The settings of VLAN, IGMP Snooping,Management VLAN, 802.1v, and MAC Address Table will be reset to default.




Success.
DES-1210-52/ME:5#
```

disable asymmetric_vlan

Purpose	To disable Asymmetric VLAN on the switch.
Syntax	**disable asymmetric_vlan**
Description	The **disable asymmetric_vlan** command, along with the **enable asymmetric_vlan** command below, is used to disable and enable Asymmetric VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable asymmetric_vlan on the switch:

```
DES-1210-52/ME:5# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.
DES-1210-52/ME:5#
```

show asymmetric_vlan

Purpose	To display the Asymmetric VLAN status on the Switch.
Syntax	**show asymmetric_vlan**
Description	The **show asymmetric_vlan** command displays the Asymmetric VLAN status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display Asymmetric VLAN status:

```
DES-1210-52/ME:5# show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN : Enable
DES-1210-52/ME:5#
```

enable pvid auto_assign

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

Example usage:

To enable the auto-assign PVID:

```
DES-1210-52/ME:5# enable pvid auto_assign
Command: enable pvid auto_assign

Success.
DES-1210-52/ME:5#
```

disalbe pvid auto_assign

Purpose	To to disable auto assignment of PVID.
Syntax	**disable pvid auto_assign**
Description	The **disable pvid auto_assign** command disables the auto-assign of PVID. When it is disabled, PVID only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID. The default setting is *enabled*.
Parameters	None.
Restrictions	Only Administrator, Operator and Power-User-level users can issue this command.

Example usage:

To disable the auto-assign PVID:

```
DES-1210-52/ME:5# disable pvid auto_assign
Command: disable pvid auto_assign

Success.
DES-1210-52/ME:5#
```

show pvid auto_assign

Purpose	To to show auto assignment of PVID.
Syntax	**show pvid auto_assign**
Description	The **show pvid auto_assign** command is used to show PVID auto-assigment state.

Parameters	None.
Restrictions	None.

Example usage:

To display the auto-assign PVID state:

```
DES-1210-52/ME:5# show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled
DES-1210-52/ME:5#
```

29

Q-IN-Q COMMANDS

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

Command	Parameter
enable qinq	
disable qinq	
show qinq	{ports [<portlist> | all]}
config qinq ports	[<portlist> | all] {role [nni | uni] | outer_tpid <hex 0x1 - 0xffff> | vlan_translation [enable | disable] | missdrop [enable | disable] | add_inner_tag [<hex 0x1 - 0xffff> | disable]}
config qinq inner_tpid	<hex 0x1-0xffff>
create vlan_translation	[<portlist> | all] [add | replace] cvid <vidlist> svid <vlanid 1-4094>
show vlan_translation	{cvid <vidlist> | ports <portlist>}
delete vlan_translation	ports [<portlist> | all] {cvid <vidlist>}

Each command is listed in detail, as follows:

enable qinq

Purpose	To enable the Q-in-Q mode.
Syntax	**enable qinq**
Description	The **enable qinq** command creates a used to enable the Q-in-Q mode. When Q-in-Q is enabled, all network port roles will be NNI port and their outer TPID will be set to 88a8. All existing static VLANs will run as SP-VLAN. All dynamically learned L2 address will be cleared. GVRP and STP need to be disabled manually. If you need to run GVRP on the Switch, firstly enable GVRP manually. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable Q-in-Q:

```
DES-1210-52/ME:5# enable qinq
Command: enable qinq



Success.
DES-1210-52/ME:5#
```

disable qinq

Purpose	To disable the Q-in-Q mode.
Syntax	**disable qinq**
Description	The **disable qinq** command creates a used to disable the Q-in-Q mode. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared, GVRP will be disabled. If you need to run GVRP on the Switch, firstly enable GVRP manually. All existing SP-VLANs will run as static 1Q VLANs. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable Q-in-Q:

```
DES-1210-52/ME:5# disable qinq
Command: disable qinq



Success.
DES-1210-52/ME:5#
```

show qinq

Purpose	To show global Q-in-Q and port Q-in-Q mode status.
Syntax	**show qinq {ports <portlist> | inner_tpid}**
Description	The **show qinq** command is used to show the global Q-in-Q status, including: port role in Q-in-Q mode and port outer TPID.
Parameters	*<portlist>* - Specifies a range of ports to be displayed. If no parameter is specified, the system will display all Q-in-Q port information. *inner_tpid* - Specifieyed.
Restrictions	None.

Example usage:

To show the Q-in-Q status for ports 1:

```
DES-1210-52/ME:5# show qinq ports 1
Command: show qinq ports 1

Port ID:   1
-----------------------------------------------------------
  Role:                          UNI
  Outer Tpid:                    0x8100
  Vlan Translation State:        Disabled
-----------------------------------------------------------
```

```
DES-1210-52/ME:5#
```

config qinq ports

Purpose	Used to configure Q-in-Q ports.
Syntax	**config qinq ports [<portlist> | all] {role [nni | uni] | outer_tpid <hex 0x1 - 0xffff> | vlan_translation [enable | disable] | missdrop [enable | disable] | add_inner_tag [<hex 0x1 - 0xffff> | disable]}**
Description	The **config qinq ports** command is used to configure the port level setting for the Q-in-Q VLAN function. This setting is not effective when the Q-in-Q mode is disabled.
Parameters	*<portlist>* - A range of ports to configure. *all* – Specifies all ports to be configure. *role* - Port role in Q-in-Q mode, it can be UNI port or NNI port. *outer_tpid* - TPID in the SP-VLAN tag. *vlan_translation* - If specified as enabled, the VLAN translation will be performed on the port. The setting is disabled by default. *missdrop [enable* | *disable]* – To enable or disable the tagged packet drop that does not match any assignment rule in the Q-in-Q profile and translated VLAN. *add_inner_tag [<hex 0x1 – 0xffff>* | *disable]* – Specifies whether to add inner tag for ingress untagged packets. Enter the inner tag value between hex 0x1 and 0xffff, or specify that only the s-tag will be added for ingress untagged packets with option-disable.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure port list 1 to 4 as NNI port, set outer TPID to 0x88a8:

```
DES-1210-52/ME:5# config qinq ports 1-4 role nni outer_tpid 0x88a8
Command: config qinq ports 1-4 role nni outer_tpid 0x88a8

Success.

DES-1210-52/ME:5#
```

config qinq inner_tpid

Purpose	Used to configure Q-in-Q inner TPID of the Switch.
Syntax	**config qinq inner_tpid <hex 0x1-0xffff>**
Description	The **config qinq inner_tpid** command is used to configure the inner TPID for port.
Parameters	<hex 0x1-0xffff> - Specifies the inner-TPID of a port.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the inner TPID to 0x88a8:

```
DES-1210-52/ME:5# config qinq inner_tpid 0x88a8
Command: config qinq inner_tpid 0x88a8

```

```
Success.

DES-1210-52/ME:5#
```

create vlan_translation

Purpose	To create a VLAN translation rule that will be added as a new rule or replace a current rule.
Syntax	**create vlan_translation [<portlist> | all] [add | replace] cvid <vidlist> svid <vlanid 1-4094>**
Description	The **create vlan_translation cvid** command is used to create a VLAN translation rule to add to or replace the outgoing packet which is single S-tagged (the C-VID changes to S-VID and the packet's TPID changes to an outer TPID).
Parameters	<*portlist*> - A range of ports to configure. *all* – Specifies all ports to be configure. *cvid* – C-VLAN ID of packets that ingress from a UNI port. *svid* – The S-VLAN ID that replaces the C-VLAN ID or is inserted in the packet. <*vlanid 1-4094*> – A VLAN ID between 1 and 4094.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a VLAN translation on the Switch:

```
DES-1210-52/ME:5# create vlan_translation ports 3-5 add cvid 2 svid 2
Command: create vlan_translation ports 3-5 add cvid 2 svid 2



Success.

DES-1210-52/ME:5#
```

show vlan_translation

Purpose	To display the current VLAN translation rules on the Switch.
Syntax	**show vlan_translation {cvid <vidlist> | ports <portlist>}**
Description	The **show vlan_translation cvid** command display the current VLAN translation cvid on the Switch
Parameters	<*vidlist*> − The Q-in-Q translation rules for the specified C-VID list. <*portlist*> - The Q-in-Q translation rules for the specified port list.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To display the VLAN translation cvid on the Switch:

```
DES-1210-52/ME:5# show vlan_translation cvid
Command: show vlan_translation cvid
```

```
CVID  SPVID  Action
------   --------  -------

Total Entries    : 0

DES-1210-52/ME:5#
```

delete vlan_translation cvid

Purpose	To delete VLAN translation rules.
Syntax	**delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}**
Description	The **delete vlan_translation cvid** command is used to delete VLAN translation rules.
Parameters	<*vidlist*> - Specifies C-VID rules in VLAN translation. <*portlist*> - The Q-in-Q translation rules for the specified port list to be deleted. *all* – Specifies all C-VID rules to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete all C-VID VLAN translation rules:

```
DES-1210-52/ME:5# delete vlan_translation ports all
Command: delete vlan_translation ports all

Success.

DES-1210-52/ME:5#
```

30

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	Parameter
create link_aggregation	group_id <value 1-8> {type [lacp | static]}
delete link_aggregation	group_id <value 1-8>
config link_aggregation group_id	<value 1-8> master_port <port 1-52> ports <portlist>
config link_aggregation algorithm	[ip_source | ip_destination | ip_source_dest | mac_source | mac_destination | mac_source_dest]
config link_aggregation state	[enable | disable]
show link_aggregation	{group_id <value 1-8> | algorithm}

Each command is listed in detail, as follows:

create link_aggregation

Purpose	To create a link aggregation group on the Switch.
Syntax	**create link_aggregation group_id <value 1-8> {type [lacp | static]}**
Description	The **create link_aggregation** command creates a link aggregation group with a unique identifier.
Parameters	*group_id* <*value 1-8*> − Specifies the group ID. The Switch allows up to 8 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. The maximum ports that can be configure in the same LACP are 16. • *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. The maximum ports that can be configure in the same static LAG are 8

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

Example usage:

To create a link aggregation group:

```
DES-1210-52/ME:5# create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DES-1210-52/ME:5#
```

delete link_aggregation

Purpose	To delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value 1-8>**
Description	The **delete link_aggregation group_id** command deletes a previously configured link aggregation group.
Parameters	*group_id <value 1-8>* − Specifies the group ID. The Switch allows up to 8 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-1210-52/ME:5# delete link_aggregation group_id 1
Command: delete link_aggregation group_id 1



LA channel 1 delete Successful
DES-1210-52/ME:5#
```

config link_aggregation group_id

Purpose	To configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-8> master_port <port 1-52> ports <portlist>**
Description	The **config link_aggregation group_id** command configures a link aggregation group created with the **create link_aggregation** command above.
Parameters	*<value 1-8>* − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *master_port <port 1-52>* − Specifies a list of ports to belong to the link aggregation group. Ports will be listed in only one aggregation group and link aggregation groups can not overlap to each other. The user must cofigure at list two ports in LAG. *ports <portlist>* − Specifies a list of ports to belong to the 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 2 with group members ports 1-5:

```
DES-1210-52/ME:5# config link_aggregation group_id 2 master_port 1 ports 1-5
Command: config link_aggregation group_id 2 master_port 1 ports 1-5

Success.
DES-1210-52/ME:5#
```

config link_aggregation algorithm

Purpose	To configure the link aggregation algorithm.
Syntax	**config link_aggregation algorithm [ip_source | ip_destination | ip_source_dest | mac_source | mac_destination | mac_source_dest]**
Description	The **config link_aggregation algorithm** command is used to configure 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	*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 and destination addresses. *mac_source* − Indicates that the Switch should examine the MAC source address. *mac_destination* − Indicates that the Switch should examine the MAC destination address. *mac_source_dest* − Indicates that the Switch should examine the MAC source and destination addresses.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure link aggregation algorithm for ip_source:

```
DES-1210-52/ME:5# config link_aggregation algorithm ip_source
Command: config link_aggregation algorithm ip_source

Success.
DES-1210-52/ME:5#
```

config link_aggregation state

Purpose	To enable or disable the link aggregation state.
Syntax	**config link_aggregation state [enable | disable]**
Description	The **config link_aggregation state** command is used to enable or disable the link algorithm feature.

Parameters	*[enable* | *disable] – Enables or disables the link aggregation state.*
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the link aggregation feature:

```
DES-1210-52/ME:5# config link_aggregation state enable
Command: config link_aggregation state enable



LA  Module has been enable
DES-1210-52/ME:5#
```

show link_aggregation

Purpose	To display the current link aggregation configuration on the Switch.
Syntax	**show link_aggregation {group_id <value 1-8> | algorithm}**
Description	The **show link_aggregation** command displays the current link aggregation configuration of the Switch.
Parameters	*group_id <value 1-8>* − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *algorithm* – shows which hash Algorithm is used for link aggregation distribution.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DES-1210-52/ME:5# show link_aggregation
Command: show link_aggregation

LA State       : Enable
Link Aggregation Algorithm = MAC_source



DES-1210-52/ME:5#
```

v

31

BASIC IP COMMANDS

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

Command	Parameter
create ipif	<ipif_name 12> <network_address> <vlan_name 32> state [enable | disable]
delete ipif	[<ipif_name 12> | all]
enable ipif	[<ipif_name 12> | all]
disable ipif	[<ipif_name 12> | all]
config ipif	<ipif_name 12> { ([ipaddress <network_address>] [vlan <vlan_name 32>] [state {enable | disable}]) | dhcp | ipv6 {ipv6address <ipv6networkaddr> | state {enable | disable}} | ipv4 state {enable | disable} | dhcp_option12 { hostname <hostname 63> | clear_hostname | state {enable | disable} } | dhcpv6_client {enable | disable} }
show ipif	<string>

Each command is listed in detail, as follows:

create ipif	
Purpose	To create an IP interface on the switch.
Syntax	**create ipif <ipif_name 12> <network_address> <vlan_name 32> state [enable | disable]**
Description	The **create ipif** command will create an IP interface.
Parameters	*<ipif_name 12>* - Specifies the IP interface name to be created. *<network_address>* - IP address and netmask of the IP interface to be created. *<vlan_name 32>* - The name of the VLAN that will be associated with the above IP interfact. *state [enable | disable]* – Specifies to enable or disable the IP interface.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create an IP interface:

```
DES-1210-52/ME:5# create ipif ip2 10.1.2.3/255.0.0.0 default state
enable
Command: create ipif ip2 10.1.2.3/255.0.0.0 default state enable


Success.
DES-1210-52/ME:5#
```

delete ipif

Purpose	To delete an IP interface on the switch.
Syntax	**delete ipif [<ipif_name 12> | all]**
Description	The **delete ipif** command will delete an IP interface.
Parameters	*[<ipif_name 12> | all]* - Specifies the IP interface name or all IP interface to be deleted.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete an IP interface:

```
DES-1210-52/ME:5# delete ipif all
Command: delete ipif all

Success.
DES-1210-52/ME:5#
```

enable ipif

Purpose	To enable an IP interface on the switch.
Syntax	**enable ipif [<ipif_name 12> | all]**
Description	The **enable ipif** command will create an IP interface.
Parameters	*[<ipif_name 12> | all]* - Specifies the IP interface name or all IP interface to be enabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable all IP interface:

```
DES-1210-52/ME:5# enable ipif all
Command: enable ipif all

Success.
DES-1210-52/ME:5#
```

disable ipif

Purpose	To disable an IP interface on the switch.
Syntax	**disable ipif [<ipif_name 12> | all]**
Description	The **disable ipif** command will create an IP interface.
Parameters	*[<ipif_name 12> | all]* - Specifies the IP interface name or all IP interface to be disabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable all IP interface:

```
DES-1210-52/ME:5# disable ipif all
Command: disable ipif all
```

```
Success.
DES-1210-52/ME:5#
```

config ipif

Purpose	To configure the DHCPv6 client state for the interface.
Syntax	**config ipif <ipif_name 12> ([ipaddress <network_address>] [vlan <vlan_name 32>] [state [enable | disable]] | dhcp | ipv6 {ipv6address <ipv6networkaddr> | state {enable | disable}} | ipv4 state [enable | disable] | dhcp_option12 { hostname <hostname 63> | clear_hostname | state [enable | disable] } | dhcpv6_client [enable | disable] }**
Description	The **config ipif system** command is used to configure the DHCPv6 client state for one interface.
Parameters	*<ipif_name 12>* − The IP interface name to be configured. The default IP Interface name on the Switch is 'System'. All IP interface configurations done are executed through this interface name. *dhcp* − Specifies the DHCP protocol for the assignment of an IP address to the Switch to use for the DHCP Protocol. *hostname <hostname 63>* – Specifies the host name of DHCP. *ipaddress <network_address>* − IP address and netmask of the IP interface to be created. The address and mask information may be specified by using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16). *gateway <ipaddr>* − IP address of gateway to be created. *state [enable* | *disable]* − Enables or disables the IP interface. ipv6 ipv6address <ipv6networkaddr> − IPv6 network address: The address should specify a host address and length of network prefix. There can be multiple V6 addresses defined on an interface. Thus, as a new address is defined, it is added on this IP interface. *dhcpv6_client [enable* | *disable]* − Enable or disable the DHCPv6 client state of the interface.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the DHCPv6 client state of the System interface to enabled:

```
DES-1210-52/ME:5# config ipif System dhcpv6_client enable
Command: config ipif System dhcpv6_client enable



Success.

DES-1210-52/ME:5#
```

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	**show ipif <string>**
Description	The **show ipif** command displays the configuration of an IP interface

	on the Switch.
Parameters	<*string*> - Specifies the IP interface name.
Restrictions	None.

Example usage:

To display IP interface settings:

```
DES-1210-52/ME:5# show ipif
Command: show ipif

IP Setting Mode                    : Static
Interface Name                     : System
Interface VLAN Name                : default
IP Address                         : 10.90.90.90
Subnet Mask                        : 255.0.0.0
Default Gateway                    : 0.0.0.0

DES-1210-52/ME:5#
```

32

BPDU ATTACK PROTECTION COMMANDS

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

Command	Parameter
config bpdu_protection ports	[<portlist> | all] [state [enable | disable] | mode [drop | block | shutdown]]
config bpdu_protection recovery_timer	[<sec 60-1000000> | infinite]
config bpdu_protection	[trap | log] [none | attack_detected | attack_cleared | both]
enable bpdu_protection	
disable bpdu_protection	
show bpdu_protection	

Each command is listed in detail, as follows:

config bpdu_protection ports

Purpose	Used to configure the BPDU Attack Protection state and mode of a port.
Syntax	**config bpdu_protection ports [<portlist> | all] [state [enable | disable] | mode [drop | block | shutdown]]**
Description	The **config bpdu_protection ports** command is used to setup the BPDU Attack Protection function for the ports on the switch. The config bpdu_protection ports command is used to configure the BPDU protection function for ports on the Switch. There are two states of BPDU attack protection function; the normal state and the under attack state. The under attack state has three modes: drop, block, and shutdown modes. A BPDU attack protection enabled port will enter under attack state when it receives an STP BPDU frame, then take action based on the configuration mode. BPDU attack protection can ONLY be used for ports that do not have STP enabled. STP for ports and BPDU attack protection on ports are not compatible. Furthermore BPDU attack protection enabled on a port effectively disables all STP function on the port. Keep in mind the following points regarding this: BPDU attack protection has a higher priority than STP BPDU forwarding (i.e. the fbpdu setting of the config stp command is enabled) when determining how to handle BPDU. That is, when fbpbu is enabled to forward STP BPDU frames AND the BPDU attack protection function is enabled, the port will not forward STP BPDU frames. BPDU attack protection has a higher priority than BPDU tunnel port setting (i.e. config bpdu_tunnel ports command) when determining

	how to handle BPDU. That is, when BPDU tunneling is enabled on a port AND the BPDU attack protection function is enabled, then BPDU tunneling is effectively disabled on the port.
Parameters	*<portlist>* – Specifies a range of ports to be configured. *all* – Specifies all ports to be configured. *state [enable* | *disable]* – Enable or disable the state of BPDU Attack Protection. The default state is disabled. *mode* – Specifies the BPDU Attack Protection mode. The modes are included: *drop* – Will drop all RX BPDU packets when the port enters under attack state. *block* – Will drop all RX packets (include BPDU and normal packets) when the port enters under attack state. *shutdown* – Will shut down the port when the port enters the under attack state. The RX BPDU Attack Protection takes effect only when the port enters under attack state while in drop and block mode.
Restrictions	Only administrator-level users can issue this command

Example usage:

To set the BPDU attack protection port state to enable and drop mode:

```
DES-1210-52/ME:5# config bpdu_protection ports 1 state enable mode drop
Command: config bpdu_protection ports 1 state enable mode drop



Success.
DES-1210-52/ME:5#
```

config bpdu_protection recovery_timer

Purpose	Used to configure the BPDU Attack Protection recovery timer.
Syntax	**config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]**
Description	The **config bpdu_protection recovery_timer** command is used to configure the auto-recovery timer. To manually recover the port, the user needs to disable and re-enable the port.
Parameters	*<sec 60-1000000>* – Specifies the recovery timer. The default value of recovery timer is 60. *infinite* – The port will not be auto recovered.
Restrictions	Only administrator-level users can issue this command

Example usage:

To configure the BPDU Attack Protection recovery timer to 120 second for the entire switch:

```
DES-1210-52/ME:5# config bpdu_protection recovery_timer 120
Command: config bpdu_protection recovery_timer 120



Success.

DES-1210-52/ME:5#
```

config bpdu_protection

Purpose	Used to configure trap and log settings for BPDU attack protection events.
Syntax	**config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]**
Description	The **config bpdu_protection** command to configure the trap and log state for BPDU attack protection and specify the type of event sent or logged.
Parameters	*trap* – Specifies the trap state. The default state is both trap and log. *log* – Specifies the log state. The default state is both trap and log. *none* – Specifies that events will not be logged or trapped for both cases. *attack_detected* – Specifies that events will be logged or trapped when a BPDU attack is detected. *attack_cleared* – Specifies that events will be logged or trapped when the BPDU attack is cleared. *both* – Specifies that events will be logged or trapped for both cases. The default setting for log is both and for trap is none.
Restrictions	Only administrator-level users can issue this command

Example usage:

To configure the BPDU Attack Protection recovery timer to 120 second for the entire switch:

```
DES-1210-52/ME:5# config bpdu_protection trap both
Command: config bpdu_protection trap both



Success.
DES-1210-52/ME:5#
```

enable bpdu_protection

Purpose	Used to globally enable BPDU attack protection on the Switch.
Syntax	**enable bpdu_protection**
Description	The **enable bpdu_protection** command is used to globally enable BPDU attack protection on the Switch. The BPDU Attack Protection function and Spanning Tree Protocol for ports are mutually exclusive. When the STP function is enabled on a particular port, BPDU Attack Protection cannot be enabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable BPDU attack protection on the entire Switch:

```
DES-1210-52/ME:5# enable bpdu_protection
Command: enable bpdu_protection



Success.
DES-1210-52/ME:5#
```

disable bpdu_protection

Purpose	Used to globally disable BPDU attack protection on the Switch.
Syntax	**disable bpdu_protection**
Description	The **disable bpdu_protection** command is Use this to disable BPDU attack protection on the entire Switch. Note that if BPDU attack protection is disabled globally, it will also be disabled for ports regardless of the config bpdu_protection ports settings.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable BPDU attack protection on the entire Switch:

```
DES-1210-52/ME:5# disable bpdu_protection
Command: disable bpdu_protection



Success.
DES-1210-52/ME:5#
```

show bpdu_protection

Purpose	Used to display BPDU attack protection settings on the Switch.
Syntax	**show bpdu_protection {ports <portlist>}**
Description	The **show bpdu_protection** command is used to view the global or per port BPDU attack protection configuration.
Parameters	*ports* – Specify to view the BPDU attack protection port configuration. *<portlist>* – Specify the ports to display. If none is specified, all ports BPDU attack protection configuration will be listed.
Restrictions	None.

Example usage:

To display global settings for BPDU protection:

```
DES-1210-52/ME:5# show bpdu_protection
Command: show bpdu_protection


  BPDU Protection Global Settings

  ---------------------------------------------------------------
BPDU Protection Status               : Enabled
BPDU Protection Recover Time    : 60 seconds
BPDU Protection Trap State         : none
BPDU Protection Log State          : none

DES-1210-52/ME:5#
```

33

ETHERNET OAM COMMANDS

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

Command	Parameter
config ethernet_oam ports	[<portlist> | all] mode [active | passive] {received_remote_loopback [ignore | process] | remote_loopback [start | stop] | state [enable | disable]}
config ethernet_oam ports	[<portlist> | all] critical_link_event [critical_event | dying_gasp] notify_state [enable | disable]
config ethernet_oam ports	[<portlist> | all] link_monitor [error_frame | error_frame_period | error_frame_seconds | error_symbol] notify_state [enable | disable] {threshold <integer 1-4294967295> | window <integer 1000-60000>}
show ethernet_oam ports	[<portlist> | all] status
show ethernet_oam ports	[<portlist> | all] configuration
show ethernet_oam ports	[<portlist> | all] statistics
show ethernet_oam ports	[<portlist> | all] event_log {index <value_list>}
clear ethernet_oam ports	[<portlist> | all] [event_log | statistics]

Each command is listed in detail, as follows:

config ethernet_oam ports	
Purpose	Used to configure Ethernet OAM mode.
Syntax	**config ethernet_oam ports [<portlist> | all] mode [active | passive] {received_remote_loopback [ignore | process] | remote_loopback [start | stop] | state [enable | disable]}**
Description	The **config ethernet_oam ports** command is used to configure ports Ethernet OAM to operate in active or passive mode. The following two actions are allowed by ports in active mode, but disallowed by ports in passive mode.
Parameters	*<portlist>* − Specifies a port or range of ports to be configured. *all* – Entering this command will set all ports on the system. *mode* – Specifies to operate in either active mode or passive mode. The default mode is active. *received_remote_loopback [ignore | process]* – Specifies the received remote loopback to be ignore or process. *remote_loopback [start | stop] – Specifies the remote loopback to be started or stopped.*

	state [enable | disable] – Specifies the state to be enabled or disabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure ports 1 to 3 to OAM mode to active:

```
DES-1210-52/ME:5# config ethernet_oam ports 1-3 mode active
Command: config ethernet_oam ports 1-3 mode active



Success.
DES-1210-52/ME:5#
```

config ethernet_oam ports

Purpose	Used to configure Ethernet OAM critical link event.
Syntax	**config ethernet_oam ports [<portlist> | all] critical_link_event [critical_event | dying_gasp] notify_state [enable | disable]**
Description	The **config ethernet_oam ports** command is used to configure ports for critical link event of Ethernet OAM.
Parameters	*<portlist>* − Specifies a port or range of ports to be configured. *all* – Entering this command will set all ports on the system. *critical_link_event [critical_event | dying_gasp]* – Specifies the critical link event is critical event or dying GASP. *notify_state [enable | disable]* – Specifies to enable or disable the event notification. The default state is enabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure ports 1 to 3 to OAM critical link event dying GASP state to be enabled:

```
DES-1210-52/ME:5# config ethernet_oam ports 1-3 critical_link_event
dying_gasp notify_state enable
Command: config ethernet_oam ports 1-3 critical_link_event
dying_gasp notify_state enable



Success.
DES-1210-52/ME:5#
```

config ethernet_oam ports

Purpose	Used to configure Ethernet OAM link monitor.
Syntax	**config ethernet_oam ports [<portlist> | all] link_monitor [error_frame | error_frame_period | error_frame_seconds | error_symbol] notify_state [enable | disable] {threshold <integer 1-4294967295> | window <integer 1000-60000>}**
Description	The **config ethernet_oam ports** command is used to configure ports link monitor of Ethernet OAM.
Parameters	*<portlist>* − Specifies a port or range of ports to be configured.

	all – Entering this command will set all ports on the system. *critical_link_event [critical_event* | *dying_gasp]* – Specifies the critical link event is critical event or dying GASP. *notify_state [enable* | *disable]* – Specifies to enable or disable the event notification. The default state is enabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure ports 1 to 3 to OAM link monitor of error symbol notify state to be disabled:

```
DES-1210-52/ME:5# config ethernet_oam ports 1-3 link_monitor error_symbol
notify_state disable
Command: config ethernet_oam ports 1-3 link_monitor error_symbol
notify_state disable



Success.
DES-1210-52/ME:5#
```

show ethernet_oam ports

Purpose	Used to show primary controls and status information for Ethernet OAM.
Syntax	**show ethernet_oam ports [<portlist> | all] status**
Description	The **show ethernet_oam ports status** command is used to show primary controls and status information for Ethernet OAM on specified ports. The information includes: (1) OAM administration status: enabled or disabled (2) OAM operation status. See below values: **Disable**: OAM is disabled on this port **LinkFault:** The link has detected a fault and is transmitting OAMPDUs with a link fault indication. **PassiveWait:** The port is passive and is waiting to see if the peer device is OAM capable. **ActiveSendLocal**: The port is active and is sending local information **SendLocalAndRemote**: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer. **SendLocalAndRemoteOk:** The local device agrees the OAM peer entity. **PeeringLocallyRejected:** The local OAM entity rejects the remote peer OAM entity. **PeeringRemotelyRejected:** The remote OAM entity rejects the local device. **Operational:** The local OAM entity learns that both it and the remote OAM entity have accepted the peering. **NonOperHalfDuplex:** Since Ethernet OAM functions are not designed to work completely over half-duplex ports. This value indicates Ethernet OAM is enabled but the port is in half-duplex operation. (3) OAM mode: passive or active (4) Maximum OAMPDU size: The largest OAMPDU that the OAM entity supports. OAM entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU

	sizes between the peers. (5) OAM configuration revision: The configuration revision of the OAM entity as reflected in the latest OAMPDU sent by the OAM entity. The config revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed. (6) OAM Functions Supported: The OAM functions supported on this port. These functions include: **Unidirectional**: It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only). **Loopback**: It indicates that the OAM entity can initiate and respond to loop-back commands. **Link Monitoring**: It indicates that the OAM entity can send and receive Event Notification OAMPDUs. **Variable**: It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB At present, only unidirectional, loop-back and link monitoring are supported.
Parameters	Specifies a port, a range of ports or all ports to be displayed.
Restrictions	None.

Example usage:

To show OAM control and status information of port 1:

```
DES-1210-52/ME:5# show ethernet_oam ports 1 status
Command: show ethernet_oam ports 1 status


Port 1
Local Client
-----------------------------------------------------------
  OAM                        : Enabled
  Mode                       : Active
  Max OAMPDU                 : 1518 Bytes
  Remote Loopback            : Support
  Unidirection               : Not Supported
  Link Monitoring            : Support
  Variable Request           : Support
  PDU Revision               : 2
  Operation Status           : Disabled
  Loopback Status            : No Loopback
DES-1210-52/ME:5#
```

show ethernet_oam ports

Purpose	Used to display for Ethernet OAM configuration.
Syntax	**show ethernet_oam ports [<portlist> | all] configuration**
Description	The **show ethernet_oam ports** command is used to show port's Ethernet OAM configurations.
Parameters	*[<portlist>* | *all]* − Specifies a port, a range of ports or all ports to be

	displayed.
Restrictions	None.

Example usage:

To show Ethernet OAM configuration of port 1:

```
DES-1210-52/ME:5# show ethernet_oam ports 1 configuration
Command: show ethernet_oam ports 1 configuration



Port 1
-----------------------------------------------------------
  OAM                                  : Enabled
  Mode                                 : Active
  Dying Gasp                           : Enabled
  Critical Event                       : Enabled
  Remote Loopback OAMPDU               : Processed

Symbol Error
  Notify State                         : Disabled
  Window                               : 1000 milliseconds
  Threshold                            : 100 Errored Symbol

Frame Error
  Notify State                        : Enabled
  Window                              : 1000 milliseconds
  Threshold                            : 1 Errored Frame

Frame Period Error
  Notify State                        : Enabled
  Window                               : 148810 Frames
  Threshold                            : 1 Errored Frame

Frame Seconds Error
  Notify State                        : Enabled
  Window                              : 60000 milliseconds
  Threshold                            : 1 Errored Seconds
DES-1210-52/ME:5#
```

show ethernet_oam ports

Purpose	Used to display for Ethernet OAM statistics.
Syntax	**show ethernet_oam ports [<portlist> | all] statistics**
Description	The **show ethernet_oam ports** command is used to show port’s Ethernet OAM statistics information.
Parameters	*[<portlist>* | *all]* − Specifies a port, a range of ports or all ports to be displayed.
Restrictions	None.

Example usage:

To show Ethernet OAM statistics of port 1:

```
DES-1210-52/ME:5# show ethernet_oam ports 1 statistics
Command: show ethernet_oam ports 1 statistics

Port 1
-----------------------------------------------------------------
  Information OAMPDU Tx                         : 0
  Information OAMPDU Rx                         : 0
  Unique Event Notification OAMPDU Tx    : 0
  Unique Event Notification OAMPDU Rx    : 0
  Duplicate Event Notification OAMPDU Tx: 0
  Duplicate Event Notification OAMPDU Rx: 0
  Loopback Control OAMPDU Tx               : 0
  Loopback Control OAMPDU Rx               : 0
  Variable Request OAMPDU Tx                : 0
  Variable Request OAMPDU Rx                : 0
  Variable Response OAMPDU Tx              : 0
  Variable Response OAMPDU Rx              : 0
  Organization Specific OAMPDUs Tx        : 0
  Organization Specific OAMPDUs Rx        : 0
  Unsupported OAMPDU Tx                     : 0
  Unsupported OAMPDU Rx                     : 0
  Frames Lost Due To OAM                    : 0
DES-1210-52/ME:5#
```

show ethernet_oam ports

Purpose	Used to display for Ethernet OAM event log.
Syntax	**show ethernet_oam ports [<portlist> | all] event_log {index <value_list>}**
Description	The **show ethernet_oam ports** command is used to show ports Ethernet OAM event log information. The Switch can buffer 1000 event logs. The event log is different from sys-log. It provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and system log.
Parameters	*[<portlist>* | *all]* − Specifies a port, a range of ports or all ports to be displayed. *index <value_list>* − Specifies an index range to display.
Restrictions	None.

Example usage:

To show port 1 external OAM event:

```
DES-1210-52/ME:5# show ethernet_oam ports 1 event_log index 1
Command: show ethernet_oam ports 1 event_log index 1



Port 1
```

```
--------------------------------------------------------------------
Event Listing
Index Type                                 Location      Time Stamp
----- ---------------------------------------- -------------    ---------------------


Local Event Statistics
  Error Symbol Event                  : 0
  Error Frame Event                   : 0
  Error Frame Period Event            : 0
  Errored Frame Seconds Event         : 0
  Dying Gasp                          : 0
  Critical Event                      : 0
Remote Event Statistics
  Error Symbol Event                  : 0
  Error Frame Event                   : 0
  Error Frame Period Event            : 0
  Errored Frame Seconds Event         : 0
  Dying Gasp                          : 0
  Critical Event                      : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

clear ethernet_oam ports

Purpose	Used to clear Ehternet OAM event log or statistics.
Syntax	**clear ethernet_oam ports [<portlist> | all] [event_log | statistics]**
Description	The **clear ethernet_oam ports** command is used to clear ports Ethernet OAM event log or statistics information.
Parameters	*[<portlist>* | *all]* − Specifies a port, a range of ports or all ports information to be cleared. *[event_log* | *statistics]* − Specifies event log or statistics information to be cleared.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To clear port 1 OAM statistics:

```
DES-1210-52/ME:5# clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics



Success.
DES-1210-52/ME:5#
```

34

MAC NOTIFICATION COMMANDS

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

Command	Parameter
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, as follows:

enable mac_notification

Purpose	Used to enable global MAC address table notification on the Switch.
Syntax	**enable mac_notification**
Description	The **enable mac_notification** 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-1210-52/ME:5# enable mac_notification
Command: enable mac_notification

Success.

DES-1210-52/ME:5#
```

disable mac_notification

Purpose	Used to disable global MAC address table notification on the Switch.
Syntax	**disable mac_notification**
Description	The **disable mac_notification** 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-1210-52/ME:5# disable mac_notification
Command: disable mac_notification

Success.

DES-1210-52/ME:5#
```

config mac_notification

Purpose	Used to configure MAC address notification.
Syntax	**config mac_notification [interval <int 1-2147483647> | historysize <int 1-500>]**
Description	The **config mac_notification** command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*interval <int 1-2147483647>* − The time in seconds between notifications. The user may choose an interval between 1 and 2147483647 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-1210-52/ME:5# config mac_notification interval 1
Command: config mac_notification interval 1

Success.

DES-1210-52/ME:5#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist> | all] [enable | disable]**
Description	The **config mac_notification ports** command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist>* − Specifies 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-1210-52/ME:5# config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-1210-52/ME:5#
```

show mac_notification

Purpose	Used to display the Switch’s MAC address table notification global settings.
Syntax	**show mac_notification**
Description	The **show mac_notification** 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-1210-52/ME:5# show mac_notification
Command: show mac_notification


Global Mac Notification Settings

State            : Enabled
Interval         : 1
History Size      : 1
DES-1210-52/ME:5#
```

show mac_notification ports

Purpose	Used to display the Switch’s MAC address table notification status settings.
Syntax	**show mac_notification ports {<portlist>}**
Description	The **show mac_notification ports** 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-1210-52/ME:5# show mac_notification ports 1-5
Command: show mac_notification ports 1-5

```

```
Port       MAC Address Table Notification State
----       ---------------------------------------------------
1                           Disabled
2                           Disabled
3                           Disabled
4                           Disabled
5                           Disabled

DES-1210-52/ME:5#
```

35

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	Parameter
config igmp_snooping	[vlan_name <string 32> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | leave_timer <sec 1-25> | fast_leave [enable | disable] | state [enable | disable]]
config igmp_snooping querier	[vlan_name <string 32> | vlanid <vidlist> | all] state [enable | disable] {querier_version [2 | 3] | last_member_query_interval <sec 1-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | max_response_time <sec 10-25>}
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 32> [add | delete] [member_port <portlist> | source_port <portlist> | tag_member_port <portlist>] state [enable | disable] {replace_source_ip [none | <ipaddr>]}
delete igmp_snooping multicast_vlan	[all | <vlan_name 32>]
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add | delete] ipv4_range <ipaddr> <ipaddr>
create igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>
delete igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
show igmp_snooping static_group	{vlan <vlan_name 32> | vlanid <vlanid_list> | <ipaddr>}
config igmp_snooping data_driven_learning	[all | vlan_name <string 32> | vlanid <vidlist>] {state [enable | disable] expiry_time <sec 130-153025> aged_out}
config igmp_snooping data_driven_learning	max_learned_entry <integer 1-256>
clear igmp_snooping data_driven_group	[all | vlan_name <vlan_name 32> | vlanid < vidlist >] [all | MCGroupAddr <ipaddr>]
config igmp_snooping max_response_time	<integer 10-25>
config router_ports	[vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>
config router_port s_forbidden	[vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>
config igmp access_authentication	[<portlist> | all] state [enable | disable]

Command	Parameter
ports	
show igmp access_authentication ports	[<portlist> | all]
enable igmp_snooping	{multicast_vlan | forward_mcrouter_only}
disable igmp_snooping	{multicast_vlan | forward_mcrouter_only}
show igmp_snooping	{vlan <vlan_name 32> | vlanid <vidlist> | multicast_vlan <vlan_name 32> | multicast_vlan_group <vlan_name 32>}
show igmp_snooping group	[vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr> {data_driven}
show igmp_snooping forwarding	{vlan <vlan_name 32> | vlanid <vidlist>}
show igmp_snooping host	{ports <portlist> | group <ipaddr> | vlan <vlan_name 32> | vlanid <vidlist>}
show igmp_snooping multicast_vlan	{<vlan_name 32>}
show igmp_snooping multicast_vlan_group	{<vlan_name 32>}
show router_port	{vlan <vlan_name 32> | vlanid <vidlist> | static | dynamic | forbidden}

Each command is listed in detail, as follows:

config igmp_snooping

Purpose	To configure IGMP snooping on the Switch.
Syntax	**config igmp_snooping [vlan_name <string 32> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | leave_timer <sec 1-25> | fast_leave [enable | disable] | state [enable | disable]]**
Description	The **config igmp_snooping** command configures IGMP snooping on the Switch.
Parameters	*vlan_name <string 32>* − The name of the VLAN for which IGMP snooping is to be configured. *vlanid <vidlist>* − The VLAN id for which IGMP snooping is to be configured. all − Specifies all VLAN for which IGMP snooping is to be configured. *host_timeout <sec 130-153025>* − 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 60-600>* − Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. *leave_timer <sec 1-25>* − Leave timer. The default is 10 seconds. *fast_leave [enable* | *disable]* − Enables or disables the fast leave.

	state [enable | *disable]* − Enables or disables IGMP snooping for the specified VLAN.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DES-1210-52/ME:5# config igmp_snooping default host_timeout 250 state enable
Command: config igmp_snooping default host_timeout 250 state enable



Success. !
DES-1210-52/ME:5#
```

config igmp_snooping querier

Purpose	To configure IGMP snooping querier on the Switch.
Syntax	**config igmp_snooping querier [vlan_name <string 32> | vlanid <vidlist> | all] state [enable | disable] {querier_version [2 | 3] | last_member_query_interval <sec 1-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | max_response_time <sec 10-25>}**
Description	The **config igmp_snooping querier** command enables IGMP snooping querier on a specific VLAN.
Parameters	*vlan_name <string 32>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 20 characters can be used. *vlanid <vidlist>* − The VLAN id for which IGMP snooping is to be configured. all − Specifies all VLAN for which IGMP snooping is to be configured. *state [enable* | *disable]* − Enables/Disables IGMP Snooping Querier. *querier_version [2* | *3]* − Specifies the IGMP Querier version on the VLAN. *last_member_query_interval [sec 1-25]* − Specifies the IGMP last member query interval on the VLAN. *query_interval [sec 60-600]* − Specifies the IGMP query interval on the VLAN. *robustness_variable [value 2-255]* − Specifies the robustness on the VLAN. *max_response_time [sec 10-25]* − Specifies the max response time on the VLAN.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DES-1210-52/ME:5# config igmp_snooping querier vlanid 2 state enable
Command: config igmp_snooping querier vlanid 2 state enable
```

```
Success. !
DES-1210-52/ME:5#
```

create igmp_snooping multicast_vlan

Purpose	To create an IGMP snooping multicast VLAN on the Switch.
Syntax	**create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>**
Description	The **create igmp_snooping multicast_vlan** command creates an IGMP snooping multicast VLAN on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping is to be created. Up to 32 characters can be used. <*vlanid 2-4094*> − The ID of the VLAN for which IGMP snooping is to be created. The range is from 2 to 4094.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a igmp snooping multicast VLAN:

```
DES-1210-52/ME:5# create igmp_snooping multicast_vlan mvln2 5
Command: create igmp_snooping multicast_vlan mvln2 5


Success.
DES-1210-52/ME:5#
```

config igmp_snooping multicast_vlan

Purpose	To configure IGMP snooping multicast VLAN on the Switch.
Syntax	**config igmp_snooping multicast_vlan <vlan_name 32> [add | delete] [member_port <portlist> | source_port <portlist> | tag_member_port <portlist>] state [enable | disable] {replace_source_ip [none | <ipaddr>]}**
Description	The **config igmp_snooping multicast_vlan** command enables IGMP snooping multicast VLAN on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping is to be configured. Up to 20 characters can be used. *[add* | *delete] − Add or delete the specified multicast VLAN of IGMP snooping.* *member_port <portlist>* − Specifies a port or a range of ports to be the member port for the multicast VLAN of IGMP snooping. *source_port <portlist>* − Specifies a port or a range of ports to be the source port for the multicast VLAN of IGMP snooping. *tag_member_port <portlist>* − Specifies a port or a range of ports to be the tagged port for the multicast VLAN of IGMP snooping. *state [enable* | *disable]* − Enables/Disables IGMP Snooping multicast VLAN. *replace_source_ip [none* | *<ipaddr>]* – Specifies the replace source IP or none.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DES-1210-52/ME:5# config igmp_snooping multicast_vlan default state enable
Command: config igmp_snooping multicast_vlan default state enable

Success.
DES-1210-52/ME:5#
```

delete igmp_snooping multicast_vlan

Purpose	To remove an IGMP snooping multicast VLAN on the Switch.
Syntax	**delete igmp_snooping multicast_vlan [all | <vlan_name 32>]**
Description	The **delete igmp_snooping multicast_vlan** command removes IGMP snooping multicast VLAN on the Switch.
Parameters	*all* − Specify all vlans to be removed. <*vlan_name 32*> − Specify the multicast vlan name to be removed on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To remove the igmp snooping multicast VLAN 'rd1':

```
DES-1210-52/ME:5# delete igmp_snooping multicast_vlan rd1
Command: delete igmp_snooping multicast_vlan rd1



Success.
DES-1210-52/ME:5#
```

config igmp_snooping multicast_vlan_group

Purpose	To specify that IGMP snooping is to be configured for multicast vlan groups on the Switch.
Syntax	**config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] ipv4_range <ipaddr> <ipaddr>**
Description	The **config igmp_snooping multicast_vlan_group** command specifies an IGMP snooping multicast VLAN group on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping is to be configured. Up to 20 characters can be used. *[add* | *delete]* − Specify whether to add or delete ports defined in the following parameter <ipaddr>. <*ipaddr*> − Specify the IP address range to be configured with the IGMP snooping multicast VLAN group.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DES-1210-52/ME:5# config igmp_snooping multicast_vlan_group
default add 10.90.90.93 10.90.90.95
Command: config igmp_snooping multicast_vlan_group default
```

```
add 10.90.90.93 10.90.90.95

Success.
DES-1210-52/ME:5#
```

create igmp_snooping static_group

Purpose	To create an IGMP snooping static group on the Switch.
Syntax	**create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>**
Description	The **create igmp_snooping static_group** command allows you to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port from the member ports of a group. The statis group will only take effect when IGMP snooping is enabled on the VLAN. For those statis member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping statis group is to be created. Up to 32 characters can be used. <*vlanid_list*> − The ID of the VLAN for which IGMP snooping static group is to be created. The range is from 2 to 4094. <*ipaddr*> − Specify the static group address for which IGMP snooping to be created.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a igmp snooping static group 226.1.1.1 for VID 1:

```
DES-1210-52/ME:5# create igmp_snooping static_group vlanid 1 226.1.1.1
Command: create igmp_snooping static_group vlanid 1 226.1.1.1




Success.
DES-1210-52/ME:5#
```

config igmp_snooping static_group

Purpose	To configure the current IGMP snooping static group on the Switch.
Syntax	**config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>**
Description	The **config igmp_snooping static_group** command is used to add or delete ports to /from the given static group.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping static group is to be configured. Up to 32 characters can be used. *[add | delete]* − Specify whether to add or delete ports defined in the

	following parameter <ipaddr>. *<ipaddr>* − Specify the IP address to be configured with the IGMP snooping static group.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To add port 5 to static group 226.1.1.1 on VID 1:

```
DES-1210-52/ME:5# config igmp_snooping static group vlanid 1 226.1.1.1 and 5



Success.DES-1210-52/ME:5#
```

delete igmp_snooping static_group

Purpose	To delete the current IGMP snooping static group on the Switch.
Syntax	**delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>**
Description	The **delete igmp_snooping static_group** command is used to delete an IGMP snooping statie group will not affect the IGMP snooping dynamic member ports of a group.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping statis group is to be created. Up to 32 characters can be used. *<vlanid_list>* − The ID of the VLAN for which IGMP snooping static group is to be created. The range is from 2 to 4094. *<ipaddr>* − Specify the static group address for which IGMP snooping to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete a static group 226.1.1.1 on VID 1:

```
DES-1210-52/ME:5# delete igmp_snooping static_group vlanid 1 226.1.1.1
Command: delete igmp_snooping static_group vlanid 1 226.1.1.1




Success.
DES-1210-52/ME:5#
```

show igmp_snooping static_group

Purpose	To display the IGMP snooping static group information on the Switch.
Syntax	**show igmp_snooping statis_group vlan <vlan_name 32> | vlanid <vlanid_list> | <ipaddr>}**
Description	The **show igmp_snooping statis_group** command displays the IGMP snooping static group information on the Switch.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping

	static group to be displayed. *<vlanid_list>* − The VLAN id of IGMP snooping static group to be displayed. *<ipaddr>* − Specify the IP address of IGMP snooping static group to be displayed.
Restrictions	None.

Example usage:

To display the IGMP snooping static group information on the Switch:

```
DES-1210-52/ME:5# show igmp_snooping static_group vlan default
Command: show igmp_snooping static_group vlan default



 VLAN ID/Name      IP Address      Static Member Ports
 ----------------------   ----------------   --------------------------------
 1      default          226.1.1.1          None

Total Entries : 1

DES-1210-52/ME:5#
```

config igmp_snooping data_driven_learning

Purpose	Used to configure the data driven learning of an IGMP snooping group.
Syntax	**config igmp_snooping data_driven_learning [all | vlan_name <string 32> | vlanid <vidlist>] {state [enable | disable] expiry_time <sec 130-153025> aged_out}**
Description	The **config igmp_snooping data_driven_learning** command configures the IGMP snooping data driven learning on the Switch.
Parameters	*all* − Specifies that all VLANs configured on the Switch will be configured. *vlan_name <string 32>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *vlanid <vidlist>* − Specify the vlan id of the IGMP snooping data driven group on the Switch. *state [enable | disable]* − Enables or Disables IGMP snooping data driven learning. *expiry_time <sec 130-153025>* − Specifies the expiry time. The range is between 130 and 153025 seconds. *aged_out* − Specifies the age out time to be enabled or diabled of IGMP snooping data driven learning.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping data driven learning on the Switch:

```
DES-1210-52/ME:5# config igmp_snooping data_driven_learning all state disable
Command: config igmp_snooping data_driven_learning all state disable
```

```


Success.DES-1210-52/ME:5#
```

config igmp_snooping data_driven_learning

Purpose	Used to configure the data driven learning of an IGMP snooping group.
Syntax	**config igmp_snooping data_driven_learning max_learned_entry <integer 1-512>**
Description	The **config igmp_snooping data_driven_learning** command configures the max learned entry of IGMP snooping data driven learning on the Switch.
Parameters	*max_learned_entry <integer 1-512>* − Specify the max learned entry, the range is from 1 to 256.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping data driven learning on the Switch:

```
DES-1210-52/ME:5#          config          igmp_snooping          data_driven_learning
max_learned_entry 10
Command: config igmp_snooping data_driven_learning max_learned_entry 10



Success.
DES-1210-52/ME:5#
```

clear igmp_snooping data_driven_group

Purpose	To clear the IGMP snooping group learned by data drive.
Syntax	**clear igmp_snooping data_driven_group [all | vlan_name <vlan_name 32> | vlanid <vidlist>] [all | MCGroupAddr <ipaddr>]**
Description	The **config igmp_snooping data_driven_learning** command is used to delete the IGMP snooping group learned by data drive. Note that this commands is currently only for layer 2 switches.
Parameters	*all* − Delete all data driven entries. *vlan_name <vlan_name 32>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 20 characters can be used. *vlanid* <vidlist> − Specify the vlan id of the IGMP snooping data driven group on the Switch. <ipaddr> - Specifies the IP address.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To clear the igmp snooping data driven group on the Switch:

```
DES-1210-52/ME:5# clear igmp_snooping data_driven_group all
```

```
Command: clear igmp_snooping data_driven_group all



Success.
DES-1210-52/ME:5#
```

config router_ports

Purpose	To configure ports as router ports.
Syntax	**config router_ports [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config router_ports** command designates a range of ports as being connected to multicast-enabled routers. This ensures all packets with such a router as its destination will reach the multicast-enabled router − regardless of protocol, etc.
Parameters	*vlan_name <string 32>* − The name of the VLAN on which the router port resides. Up to 20 characters can be used. *vlanid <vidlist>* − The VLAN id of the VLAN on which the router port resides. *all* − Specifies all ports on the Switch to be configured. *[add | delete]* – Specifies whether to add or delete ports defined in the following parameter <portlist>, to the router port function. *<portlist>* − A port or range of ports that will be configured as router ports.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To add the static router ports 1-5:

```
DES-1210-52/ME:5# config router_ports vlanid 1 add 1-5
Command: config router_ports vlanid 1 add 1-5



Success.
DES-1210-52/ME:5#
```

config router_ports_forbidden

Purpose	To deny ports becoming router ports.
Syntax	**config router_ports_forbidden [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config router_port_forbidden** command denies a range of ports access to multicast–enabled routers. This ensures all packets with such a router as its destination will not reach the multicast–enabled router − regardless of protocol, etc.
Parameters	*vlan_name <string 32>* − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *vlanid <vidlist>* − The VLAN id of the VLAN on which the router port resides.

	all − Specifies all ports on the Switch to be configured. *[add | delete]* – Specifies whether to deny ports defined in the following parameter <portlist>, to the router port function. *<portlist>* − A port or range of ports that will be denied access as router ports.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To deny router ports:

```
DES-1210-52/ME:5# config router_ports_forbidden vlanid 2 add 10-12
Command: config router_ports_forbidden vlanid 2 add 10-12



Success.
DES-1210-52/ME:5#
```

config igmp access_authentication ports

Purpose	To configure the IGMP access authentication on the Switch.
Syntax	**config igmp access_authentication ports [<portlist> | all] state [enable | disable]**
Description	The **config igmp access_authentication ports** command configures the IGMP access authentication on the Switch.
Parameters	*<portlist>* − A port or range of ports that will be configured as IGMP access authentication ports. *all* − Specify all ports to be configured as IGMP access authentication ports. *State [enable | disable]* − Specifies the state for the port to be disabled or enabled.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To configure authentication port of IGMP:

```
DES-1210-52/ME:5# config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable



Success.
DES-1210-52/ME:5#
```

show igmp access_authentication ports

Purpose	To display the IGMP access authentication configuration on the Switch.
Syntax	**show igmp access_authentication ports [<portlist> | all]**
Description	The **show igmp access_authentication** command displays the IGMP access authentication configuration on the Switch.
Parameters	*all* − Specifies all ports to be displayed.

	<portlist> − A port or range of ports to be displayed on the Switch.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To display the IGMP access authentication:

```
DES-1210-52/ME:5# show igmp access_authentication ports 1-5
Command: show igmp access_authentication ports 1-5

Port   Authentication State
------ ----------------------------------
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled

DES-1210-52/ME:5#
```

enable igmp_snooping

Purpose	To enable IGMP snooping on the Switch.
Syntax	**enable igmp_snooping {multicast_vlan | forward_mcrouter_only}**
Description	The **enable igmp_snooping** command enables IGMP snooping on the Switch.
Parameters	*{multicast_vlan* | *forward_mcrouter_only}* − Enables the multicast VLAN or forward mcrouter for IGMP Snooping on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DES-1210-52/ME:5# enable igmp_snooping
Command: enable igmp_snooping

Success.
DES-1210-52/ME:5#
```

disable igmp_snooping

Purpose	To disable IGMP snooping on the Switch.
Syntax	**disable igmp_snooping {multicast_vlan | forward_mcrouter_only}**
Description	The **disable igmp_snooping** 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	*{multicast_vlan* | *forward_mcrouter_only}* − Disables the multicast

	VLAN or forward mcrouter for IGMP Snooping on the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

TTo disable IGMP snooping on the Switch:

```
DES-1210-52/ME:5# disable igmp_snooping
Command: disable igmp_snooping


Success.
DES-1210-52/ME:5#
```

show igmp_snooping

Purpose	To show the current status of IGMP snooping on the Switch.
Syntax	**show igmp_snooping {vlan <vlan_name 32> | vlanid <vidlist> | multicast_vlan <vlan_name 32> | multicast_vlan_group <vlan_name 32>}**
Description	The **show igmp_snooping** command displays the current IGMP snooping configuration on the Switch.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 32 characters can be used. *<vidlist>* − The vid of the VLAN for which IGMP snooping configuration is to be displayed.
Restrictions	None.

Example usage:

To show igmp snooping:

```
DES-1210-52/ME:5# show igmp_snooping vlan default
Command: show igmp_snooping vlan default


 IGMP Snooping Global State      : Enable
 Max Learned Entry Value         : 512
 Forward Router Only             : Disable

 VLAN Name                       : default
 Query Interval                  : 125
 Max Response Time               : 10
 Robustness Value                : 2
 Last Member Query Interval      : 1
 Querier State                   : Disable
 Querier Role                    : Non-Querier
 Querier IP                      : 0.0.0.0
 Querier Expiry Time             : 0
 State                           : Enable
 Fast Leave                      : Disable
 Report Suppression              : Enable
 Version                          : 2
 Data Driven Learning Aged Out : Disable
 Data Driven Learning State       : Disable

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

show igmp_snooping group

Purpose	To display the current IGMP snooping group configuration on the Switch.
Syntax	**show igmp_snooping group [vlan <vlan_name 32> | vlanid <vidlist> | ports <portlist>] <ipaddr> {data_driven}**
Description	The **show igmp_snooping group** command displays the current IGMP snooping group configuration on the Switch.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN for which IGMP snooping group configuration information is to be displayed. Up to 20 characters can be used. *vlanid <vidlist>* − The ID of the VLAN for which IGMP snooping group configuration infor mation is to be displayed. *ports <portlist>* − The ports of the VLAN for which IGMP snooping group configuration infor mation is to be displayed. *<ipaddr>* − Specifies to display the IP address of IGMP snooping group. *{data_driven}* − Specifies to display the data driven of IGMP snooping group.
Restrictions	None.

Example usage:

To show igmp snooping group:

```
DES-1210-52/ME:5# show igmp_snooping group vlan default
Command: show igmp_snooping group vlan default

Total Entries : 0

DES-1210-52/ME:5#
Reports          : 1
Port Member     : 3,4

Total Entries     : 1

DES-1210-52/ME:5#
```

show igmp_snooping forwarding

Purpose	To display the IGMP snooping forwarding table entries on the Switch.
Syntax	**show igmp_snooping forwarding {vlan <vlan_name 32> | vlanid <vidlist>}**
Description	The **show igmp_snooping forwarding** command displays the

	current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN for which IGMP snooping forwarding table information is to be displayed. Up to 20 characters can be used. *vlanid <vidlist>* − The vid of the VLAN for which IGMP snooping forwarding table information is to be displayed.
Restrictions	None.

Example usage:

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

```
DES-1210-52/ME:5# show igmp_snooping forwarding vlan Trinity
Command: show igmp_snooping forwarding vlan Trinity



Total Entries : 0
DES-1210-52/ME:5#
```

show igmp_snooping host

Purpose	To display the IGMP snooping host table entries on the Switch.
Syntax	**show igmp_snooping host {ports <portlist> | group <ipaddr> | vlan <vlan_name 32> | vlanid <vidlist>}**
Description	The **show igmp_snooping host** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*ports <portlist>* − The ports of IGMP snooping host table information are to be displayed. *group <ipaddr>* − The IP address of IGMP snooping host table information are to be displayed. *vlan <vlan_name 32>* − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be used. *vlanid <vidlist>* − The vid of the VLAN for which IGMP snooping host table information is to be displayed.
Restrictions	None.

Example usage:

To view the IGMP snooping host table on the Switch:

```
DES-1210-52/ME:5# show igmp_snooping host
Command: show igmp_snooping host

VLAN ID    Group                 Port No      IGMP Host
 ----------   --------------------  -------------   ------------



Total Entries : 0

DES-1210-52/ME:5#
```

show igmp_snooping multicast_vlan

Purpose	To display the IGMP snooping multicast vlan table entries on the Switch.
Syntax	**show igmp_snooping multicast_vlan {<vlan_name 32>}**
Description	The **show igmp_snooping multicast_vlan** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be used.
Restrictions	None.

Example usage:

To view the IGMP snooping multicast vlan information on the Switch:

```
DES-1210-52/ME:5# show igmp_snooping multicast_vlan default
Command: show igmp_snooping multicast_vlan default

Multicast VLAN Global State : Disabled



DES-1210-52/ME:5#
```

show igmp_snooping multicast_vlan_group

Purpose	To display the IGMP snooping multicast vlan group table entries on the Switch.
Syntax	**show igmp_snooping multicast_vlan_group {<vlan_name 32>}**
Description	The **show igmp_snooping multicast_vlan_group** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be used.
Restrictions	None.

Example usage:

To view the IGMP snooping multicast vlan group information on the Switch:

```
DES-1210-52/ME:5# show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group

VID  Vlan Name                       IP Range
---- ------------------------------- -----------------------------------------



DES-1210-52/ME:5#
```

show router_ports

Purpose	To display the currently configured router ports on the Switch.
Syntax	**show router_ports {vlan <vlan_name 32> | vlanid <vidlist> | static | dynamic | forbidden}**
Description	The **show router_ports** command displays the router ports currently configured on the Switch.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN on which the router port resides. Up to 20 characters can be used. *vlanid <vidlist>* − The ID 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 learned. *forbidden* − Displays router ports that have been forbidden configured.
Restrictions	None.

Example usage:

To display the router ports.

```
DES-1210-52/ME:5# show router_ports
Command: show router_ports

VLAN Name              : default
Static router port     :
Dynamic router port    :
Forbidden router port :

Total Entries : 1
DES-1210-52/ME:5#
```

36

DIGITAL DIAGNOSTIC MONITORING COMMANDS

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

Command	Parameter
config ddm ports	<portlist> [bias_current_threshold [high_alarm | low_alarm] | rx_power_threshold | shutdown | state [enable | disable] | temperature_threshold | tx_power_threshold | voltage_threshold]
config ddm power_unit	[mw | dbm]
show ddm ports	<portlist> [configuration | status | vendor_info]

Each command is listed in detail, as follows:

config ddm ports	
Purpose	To configure the DDM settings of the specified ports.
Syntax	**config ddm ports <portlist> [bias_current_threshold [high_alarm | low_alarm] | rx_power_threshold | shutdown | state [enable | disable] | temperature_threshold | tx_power_threshold | voltage_threshold]**
Description	The **config ddm ports** command is used to configure the DDM settings of the specified ports.
Parameters	*<portlist>* - Specifies the range of ports to be configured. *bias_current_threshold* - Specify the threshold of the optic module's bias current. *high_alarm* - Specify the high threshold for the alarm. When the operating parameter rises above this value, the action associated with the alarm is taken *low_alarm* -Specify the low threshold for the alarm. When the operating parameter falls below this value, the action associated with the alarm is taken. *rx_power_threshold* - Specify the threshold of optic module's received power.. *state* - Specify the DDM state to enable or disable. If the state is disabled, no DDM action will take effect. *temperature_threshold* - Specify the threshold of the optic module's temperature in centigrade. At least one parameter shall be specified for this threshold. *shutdown* - Specify whether or not to shutdown the port when the operating parameter exceeds the corresponding alarm threshold or warning threshold. The default value is none. *tx_power_threshold* - Specify the threshold of the optic module's output power. *voltage_threshold* - Specify the threshold of optic module's voltage.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the port 21's voltage threshold:

```
DES-1210-52/ME:5# config ddm ports 1:21 temperature_threshold
high_alarm 84.9555 low_alarm -10 high_warning 70 low_warning
2.25251
Command: config ddm ports 1:21 temperature_threshold high_alarm
84.9555 low_alarm -10 high_warning 70 low_warning 2.25251

Success.

DES-1210-52/ME:5#
```

config ddm power_unit

Purpose	To configure the unit of DDM TX and RX power.
Syntax	**config ddm power_unit [mw | dbm]**
Description	The **config ddm power_unit** command is used to configure the unit of DDM TX and RX power.
Parameters	*mw* - Specify the DDM TX and RX power unit as mW. *dbm* - Specify the DDM TX and RX power unit as dBm.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the DDM TX and RX power unit as dBm:

```
DES-1210-52/ME:5# config ddm power_unit dbm
Command: config ddm power_unit dbm




Success.
DES-1210-52/ME:5#
```

show ddm ports

Purpose	To display the current operating DDM parameters and configuration values of the optic module of the specified ports.
Syntax	**show ddm ports <portlist> [configuration | status | vendor_info]**
Description	The **config ddm power_unit** command is used to display the current operating DDM parameters and configuration values of the optic module of the specified ports.
Parameters	*<portlist>* - Specify the ports of DDM to be displayed. *configuration* - Specifies that the configuration values will be displayed. *status* - Specifies that the operating parameter will be displayed. vendor_info - Specifies that the vender information will be displayed.
Restrictions	None.

Example usage:

To display ports 1-5's operating parameters:

```
DES-1210-52/ME:5# show ddm ports 1-5 vender_info
Command: show ddm ports 1-5 vender_info

Invalid DDM port list.

Failure!
DES-1210-52/ME:5#
```

37

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	Parameter
enable mld_snooping	{multicast_vlan | forward_mcrouter_only}
disable mld_snooping	{multicast_vlan | forward_mcrouter_only}
config mld_snooping	[vlan_name <string 32> | vlanid <vidlist> | all] {fast_done [enable | disable] | host_timeout <sec 130-1530255> | leave_timer <sec 1-25> | router_timeout <sec 60-600> | state [enable | disable] | report_suppression [enable | disable]}
create mld_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config mld_snooping multicast_vlan	<vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 <ipv6addr> | remap_priority [<value 0-7> | none] { replace_priority}}
show mld_snooping multicast_vlan	<vlan_name 32>
delete mld_snooping multicast_vlan	[<vlan_name 32> | all]
config mld_snooping multicast_vlan_group	<vlan_name 32> [add | delete] ipv6_range <ipv6addr> <ipv6addr>
show mld_snooping multicast_vlan_group	{<vlan_name 32>}
config mld_snooping mrouter_ports	[vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>
config mld_snooping mrouter_port_forbidden	[vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>
config mld_snooping querier	[vlan_name <string 32> | vlanid <vidlist> | all] [last_listener_query_interval <sec 1-25> | max_response_time <sec 10-25> | query_interval <sec 60-600> | robustness_variable | state [enable | disable] | version <value 1-2>]
config mld_snooping data_driven_learning	[max_learned_entry <value 1-256>| vlan_name <string 32> | vlanid <vidlist> | all] [age_out [disable | enable] | expiry_time <sec 130-1530255> | state [enable | disable]]
clear mld_snooping data_driven_group	[vlan_name <string> | vlanid <vidlist> | all] {<ipv6_addr> | all}
show mld snooping	[vlan_name <string 32> | vlanid <vidlist> | all]
show mld_snooping forwarding	[vlan_name <string 32> | vlanid <vidlist> | all]
show mld_snooping group	[vlan_name <string 32> | vlanid <vidlist> | all | ports <portlist>]

Command	Parameter
show mld_snooping mrouter_ports	[vlan_name <string 32> | vlanid <vidlist> | all] [dynamic | static]
show mld_snooping host	[vlan_name <string 32> | vlanid <vidlist> | all | ports <portlist> | group <ipv6_addr>]

Each command is listed in detail, as follows:

enable mld_snooping

Purpose	To enable MLD snooping on the Switch.
Syntax	**enable mld snooping {multicast_vlan | forward_mcrouter_only}**
Description	The **enable mld snooping** command enables MLD snooping on the Switch.
Parameters	*{multicast_vlan | forward_mcrouter_only}* − Enables the multicast VLAN or forward mcrouter for MLD Snooping on the Switch.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To enable the MLD snooping:

```
DES-1210-52/ME:5# enable mld_snooping
Command: enable mld_snooping



Success.
DES-1210-52/ME:5#
```

disable mld_snooping

Purpose	To disable MLD snooping on the Switch.
Syntax	**disable mld snooping {multicast_vlan | forward_mcrouter_only}**
Description	The **disable mld snooping** command disables MLD snooping on the Switch.
Parameters	*{multicast_vlan | forward_mcrouter_only}* − Disables the multicast VLAN or forward mcrouter for MLD Snooping on the Switch.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To disable the MLD snooping:

```
DES-1210-52/ME:5# disable mld_snooping
Command: disable mld_snooping



Success.
DES-1210-52/ME:5#
```

config mld_snooping

Purpose	To configure mld snooping.
Syntax	**config mld_snooping [vlan_name <string 32> | vlanid <vidlist> | all] {fast_done [enable | disable] | host_timeout <sec 130-1530255> | leave_timer <sec 1-25> | router_timeout <sec 60-600> | state [enable | disable] | report_suppression [enable | disable]}**
Description	The **config mld_snooping** command defines mld snooping on the VLAN.
Parameters	*vlan_name <string 32>* – *S*pecifies that the mld snooping applies only to this previously created VLAN. vlanid <vidlist> – Specifies that the mld snooping applies only to this VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *fast_done [enable* | *disable]* – Specifies the fast down to be enabled or disabled. *host_timeout <sec 130-1530255>* – 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. *leave_timer <sec 1-25>* – Specifies the maximum amount of time a host can be a member of a multicast group after sending a done timer membership report. The default is 10 seconds. *router_timeout <sec 60-600>* – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report done timer. The default is 300 seconds. *state [enable* | *disable]*– Allows the user to enable or disable MLD snooping for the specified VLAN. report_suppression [enable | disable] -
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To configure mld snooping:

```
DES-1210-52/ME:5# config mld_snooping vlan_name default fast_done disable host_timeout 130 leave_timer 3 router_timeout 60 state enable
Command: config mld_snooping vlan_name default fast_done disable host_timeout 130 leave_timer 3 router_timeout 60 state enable



Success.
DES-1210-52/ME:5#
```

create mld_snooping multicast_vlan

Purpose	To create an MLD multicast VLAN.
Syntax	**create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>**
Description	The **config mld_snooping multicast_vlan** command will create a

	MLD multicast_vlan. Multiple multicast VLANs can be configured. When creating MLD multicast VLAN, it cannot duplicate with the VLAN entries in the existing 802.1Q VLAN database. The MLD Multicast VLAN snooping function co-exists with the 1Q VLAN snooping function.
Parameters	<*vlan_name 32*> − The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 20 characters. *vlanid* – The VLAN ID of the multicast VLAN to be create. The range is 2-4094.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To create mld snooping multicast VLAN mv1:

```
DES-1210-52/ME:5# create mld_snooping multicast_vlan mv1 2
Command: create mld_snooping multicast_vlan mv1 2

Success.
DES-1210-52/ME:5#
```

config mld_snooping multicast_vlan

Purpose	To configure an MLD multicast VLAN.
Syntax	**config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 <ipv6addr> | remap_priority [<value 0-7> | none] { replace_priority}}**
Description	The **config mld_snooping multicast_vlan** command allows you to add an untagged member port, a tagged member port, a untagged source port and a tagged source port to the port list. The untagged member port and the untagged source port will automatically become the untagged members of the multicast VLAN, the tagged member port and the tagged source port will automatically become the tagged members of the multicast VLAN. To change the port list, the Switch will add or delete the port list that user entered, and update the previous port list. The member port list and source port list cannot overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN. Before configuring the multicast VLAN member port by using this command, the multicast VLAN must be created first.
Parameters	<*vlan_name 32*> − The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 20 characters. *member_port* – Adds a range of member ports to the multicast VLAN. They will become the untagged member port of the MLD multicast VLAN. *source_port* – Adds a range of source ports to the multicast VLAN. *untag_source_port* – Adds a range of untagged source ports to the multicast VLAN.The PVID of the untag source port will be automatically changed to the multicast VLAN. It shall be only one kind of source port, tag or untag for an ISM VLAN. *tag_member_port* – Specifies the tagged member port of the MLD multicast VLAN. *state* – enable or disable multicast VLAN for the chosen VLAN.

	replace_source_ipv6 <ipv6addr> – With the MLD snooping function, the MLD report packet sent by the host will be forwarded to the source port. Before the forwarding of the packet, the source IP address in the join packet needs to be replaced by this IPv6 address. *remap_priority* – Associates the remap priority value (*0* to *7*) with the data traffic and is forwarded on the multicast VLAN. If *none* is specified, the packet's original priority will be used.The default setting is *none*.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To config MLD multicast VLAN mv1:

```
DES-1210-52/ME:5# config mld_snooping multicast_vlan mv1 add member_port
1,3 state enable
Command: config mld_snooping multicast_vlan mv1 add member_port 1,3 state
enable


Success.
DES-1210-52/ME:5#
```

show mld_snooping multicast_vlan

Purpose	To to show the information of MLD multicast VLAN.
Syntax	**show mld_snooping multicast_vlan <vlan_name 32>**
Description	The **show mld_snooping multicast_vlan** command allows user to show the information of an MLD multicast VLAN.
Parameters	*<vlan_name 32>* – specifies that the mld snooping applies only to this previously created VLAN.
Restrictions	None.

Example usage:

To show MLD multicast VLAN:

```
DES-1210-52/ME:5# show mld_snooping multicast_vlan mv1
Command: show mld_snooping multicast_vlan mv1

Multicast VLAN Global State : Enabled
DES-1210-52/ME:5#
```

delete mld_snooping multicast_vlan

Purpose	To to delete an MLD muticast VLAN.
Syntax	**delete mld_snooping multicast_vlan [<vlan_name 32> | all]**
Description	The **delete mld_snooping multicast_vlan** command allows user to delete an MLD multicast VLAN.
Parameters	*[<vlan_name 32>* | *all]* – *S*pecifies the name or all multicast VLAN to be deleted.
Restrictions	Only administrator, operator or power user–level users can issue

	this command.

Example usage:

To delete a MLD multicast VLAN:

```
DES-1210-52/ME:5# delete mld_snooping multicast_vlan mv1
Command: delete mld_snooping multicast_vlan mv1

Success.
DES-1210-52/ME:5#
```

config mld_snooping multicast_vlan_group

Purpose	To bind a multicast group profile to a multicast VLAN. The binding profile will affect the group joined to the multicast VLAN.
Syntax	**config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] ipv6_range <ipv6addr> <ipv6addr>**
Description	After binding a profile to a multicast VLAN, when a multicast group attempt to join this multicast VLAN member port, the group cannot join this multicast VLAN if the group does not belong to the range of binding profile.
Parameters	<*vlan_name 32*> − The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 20 characters. *add* − Used to associate a profile to a multicast VLAN. *delete* − Used to de-associate a profile from a multicast VLAN. *ipv6_range <ipv6addr>* − Specified the IPv6 address range.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To configure mld snooping multicast VLAN group mv2:

```
DES-1210-52/ME:5# config mld_snooping multicast_vlan_group mv2 add
ipv6_range 3000::1 3000::3
Command: config mld_snooping multicast_vlan_group mv2 add ipv6_range
3000::1 3000::3

Success.
DES-1210-52/ME:5#
```

show mld_snooping multicast_vlan_group

Purpose	To display the multicast group profiles configured for the specified MLD multicast VLAN.
Syntax	**show mld_snooping multicast_vlan_group {<vlan_name 32>}**
Description	After binding a profile to a multicast VLAN, when a multicast group attempt to join this multicast VLAN member port, the group cannot join this multicast VLAN if the group does not belong to the range of binding profile.
Parameters	<*vlan_name 32*> − Specifies the name of multicast VLAN to be displayed.
Restrictions	None.

Example usage:

To display mld snooping multicast VLAN group:

```
DES-1210-52/ME:5# show mld_snooping multicast_vlan_group
Command: show mld_snooping multicast_vlan_group

VID  Vlan Name                    IP Range
---- ------------------------------ ---------------------------------------


DES-1210-52/ME:5#
```

config mld_snooping mrouter_ports

Purpose	To enable mld mrouter ports.
Syntax	**config mld_snooping mrouter_ports [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config mld_snooping mrouter_ports** command defines a port that is connected to a multicast router port.
Parameters	*vlan_name <string 32>* – specifies that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *add* – Adds a specified port to the mld snooping mrouter port. *delete* – Deletes a specified port to the mld snooping mrouter port. <*portlist*> – Defines the ports to be included from the mld snooping mrouter group.
Restrictions	Only administrator, operator or power user–level users can issue this command. Separate non–consecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports. These ports are defined as connected to a multicast router.

Example usage:

To configure mld mrouter ports:

```
DES-1210-52/ME:5# config mld_snooping mrouter_ports vlanid 1 add 1-3
Command: config mld_snooping mrouter_ports vlanid 1 add 1-3



Success.
DES-1210-52/ME:5#
```

config mld_snooping mrouter_port_forbidden

Purpose	To define mld mrouter ports forbidden on the Switch.
Syntax	**config mld_snooping mrouter_port_forbidden [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config mld_snooping mrouter_port_forbidden** command forbids a port from being defined as a multicast router port by static configuration or by automatic learning.
Parameters	*vlan_name <string 32>* – Specifies that the mld snooping applies

	only to this previously created VLAN. *vlanid <vidlist>* – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *add* – Adds a specified port to the mld snooping mrouter port*.* *delete* – Deletes a specified port to the mld snooping mrouter port*.* *<portlist>* – Defines the ports to be included from the mld snooping mrouter group.
Restrictions	Only administrato–level users can issue this command.

Example usage:

To define the MLD snooping mrouter forbidden:

```
DES-1210-52/ME:5# config mld_snooping mrouter_ports_forbidden vlanid
1 add 8
Command: config mld_snooping mrouter_ports_forbidden vlanid 1 add 8



Success.
DES-1210-52/ME:5#
```

config mld_snooping querier

Purpose	Used to configure the timers and settings for the MLD snooping querier for the Switch.
Syntax	**config mld_snooping querier [vlan_name <string 32> | vlanid <vidlist> | all] [last_listener_query_interval <sec 1-25> | max_response_time <sec 10-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | state [enable | disable] | version <value 1-2>]**
Description	The **config mld_snooping querier** command allows users to configure the time between general query transmissions, the maximum time to wait for reports from listeners and the permitted packet loss guaranteed by MLD snooping.
Parameters	*vlan_name <string 32>* – Specifies that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *last_listener_query_interval <sec 1-25>* – The maximum amount of time to be set between group-specific query messages. This interval may be reduced to lower the amount of time it takes a router to detect the loss of a last listener group. The user may set this interval between 1 and 25 seconds with a default setting of 1 second. *max_response_time <sec 10-25>* – The maximum time to wait for reports from listeners. The user may specify a time between 1 and 25 seconds with a default setting of 10 seconds. *query_interval <sec 60-600>* – Specifies the amount of time between general query transmissions. The user may specify a time between 1 and 65535 seconds with a default setting of 125 seconds. *robustness_variable <value 2-255>* – Provides fine-tuning to allow

	for expected packet loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If a subnet is expected to be lossy, the user may wish to increase this interval. *state [enable | disable]* – Enabling the querier state will set the Switch as a MLD querier and disabling it will set it as a Non-querier. The default setting is disabled. *version <value 1-2>* – Specify the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be forward from router ports or VLAN flooding. The value is between 1 and 2.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To configure MLD snooping querier:

```
DES-1210-52/ME:5#config mld_snooping querier all last_listener_query_interval
1 max_response_time 10 query_interval 60 robustness_variable 2 state disable
version 1
Command: config mld_snooping querier all last_listener_query_interval 1
max_response_time 10 query_interval 60 robustness_variable 2 state disable
version 1



Success.
DES-1210-52/ME:5#
```

config mld_snooping data_driven_learning

Purpose	To enable or disable the data-driven learning of an MLD snooping group on the Switch.
Syntax	**config mld_snooping data_driven_learning [max_learned_entry <value 1-512>| vlan_name <string 32> | vlanid <vidlist> | all] [age_out [disable | enable] | expiry_time <sec 130-1530255> | state [enable | disable]]**
Description	The **config mld_snooping data driven_learning** command used to enable or disable the data-driven learning of an MLD snooping group.
Parameters	*max_learned_entry <value 1-512>* – Specifies the maximum learned entry value. *vlan_name <string 32>* – Specifies that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – *S*pecifies that the mld snooping applies only to this previously created VLAN id. *all* – Specifies that MLD snooping is to be configured for all VLANs on the Switch. *age_out [disable | disable]* –Enable or disable the aging out of entries. By default, the state is disabled. *expiry_time <sec 130-1530255>* –Specify the data driven group lifetime, in seconds. The value is between 130 and 1530255. *state [enable | disable]* –Specify to enable or disable the data driven learning of MLD snooping groups.
Restrictions	Only administrator–level users can issue this command.

Example usage:

To enable the data driven learning of an MLD snooping group on the default VLAN:

```
DES-1210-52/ME:5# config mld_snooping data_driven_learning vlan_name default state enable
Command: config mld_snooping data_driven_learning vlan_name default state enable



Success. !
DES-1210-52/ME:5#
```

clear mld_snooping data_driven_group

Purpose	To clear the mld snooping data driven group on the Switch.
Syntax	**clear mld_snooping data_driven_group [vlan_name <string 32> | vlanid <vidlist> | all] {<ipv6_addr> | all}**
Description	The **clear mld_snooping data_driven_group** command used to clear the mld snooping data driven group on the Switch.
Parameters	*vlan_name <string 32>* – Clear that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – Clear that the mld snooping applies only to this previously created VLAN id. *all* – Clear that MLD snooping is to be configured for all VLANs on the Switch. *{<ipv6_addr> | al}l* – Specifies the IPv6 address or all of mld snooping data driven group to be removed.
Restrictions	Only administrator–level users can issue this command.

Example usage:

To clear MLD snooping data driven group:

```
DES-1210-52/ME:5# clear mld_snooping data_driven_group vlan_name 2 3000::1
Command: clear mld_snooping data_driven_group vlan_name 2 3000::1



Success. !
DES-1210-52/ME:5#
```

show mld_snooping

Purpose	To display mld snooping settings on the Switch.
Syntax	**show mld_snooping [vlan_name <string 32> | vlanid <vidlist> | all]**
Description	The **show mld snooping** command displays a port from being defined as a multicast router port by static configuration or by automatic learning.
Parameters	*vlan_name <string 32>* – Displays that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – Displays that the mld snooping applies only to this previously created VLAN id.

	all – Displays that MLD snooping which configured for all VLANs on the Switch.
Restrictions	None.

Example usage:

To show the MLD snooping:

```
DES-1210-52/ME:5# show mld_snooping vlan_name default
Command: show mld_snooping vlan_name default



 MLD Snooping Global State         : Enable
 Max Learned Entry Value           : 512

 VLAN Name                         : default
 Query Interval                    : 125
 Max Response Time                 : 10
 Robustness Value                  : 2
 Last Member Query Interval        : 1
 Querier State                     : Disable
 Querier Role                      : Non-Querier
 Querier Select                    : Enable
 Querier IP                        :
 Querier Expiry Time               : 0
 State                             : Disable
 Fast Leave                        : Disable
 Version                           : 2
 Data Driven Learning Aged Out     : Disable


Total Entries : 1

DES-1210-52/ME:5#
```

show mld_snooping forwarding

Purpose	To display mld snooping settings on the Switch.
Syntax	**show mld_snooping forwarding [vlan_name <string 32> | vlanid <vidlist> | all]**
Description	The **show mld_snooping forwarding** command displays the current MLD snooping forwarding table entries currently configured on the Switch.
Parameters	*vlan_name <string 32>* – Displays that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch.
Restrictions	None.

Example usage:

To display the MLD snooping forwarding:

```
DES-1210-52/ME:5# show mld_snooping forwarding all
Command: show mld_snooping forwarding all



Total Entries : 0
DES-1210-52/ME:5#
```

show mld_snooping group

Purpose	To display mld snooping group settings on the Switch.
Syntax	**show mld_snooping group [vlan_name <string 32> | vlanid <vidlist> | all | ports <portlist>]**
Description	The **show mld_snooping group** command displays the multicast groups that were learned by MLD snooping.
Parameters	*vlan_name <string 32>* – The name of the VLAN for which to view the MLD snooping group configurations. *vlanid <vidlist>* – The id of the VLAN for which to view the MLD snooping group configurations. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch. *ports <portlist>* – The ports of the VLAN for which to view the MLD snooping group configurations.
Restrictions	None.

Example usage:

To show the MLD snooping groups:

```
DES-1210-52/ME:5# show mld_snooping group all
Command: show mld_snooping group all



Total Entries : 0

DES-1210-52/ME:5#
```

show mld_snooping mrouter_ports

Purpose	To display information on dynamically learnt and static multicast router interfaces.
Syntax	**show mld_snooping mrouter_ports [vlan_name <string 32> | vlanid <vidlist> | all] [dynamic | static]**
Description	The **show mld_snooping mrouter_port** command displays on dynamically learnt and static multicast router interfaces.
Parameters	*vlan_name <string 32>* – Specifies on which VLAN mld snooping groups should be shown. *vlanid <vidlist>* – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that all MLD snooping which configured for all VLANs

	on the Switch. *static* − Displays statically configured MLD router ports. *dynamic* − Displays dynamically configured MLD router ports.
Restrictions	None.

Example usage:

To show the MLD_snooping mrouterport:

```
DES-1210-52/ME:5# show mld_snooping mrouter_ports vlanid 1 static
Command: show mld_snooping mrouter_ports vlanid 1 static

VLAN Name           : default
Static router port  : 1-3

Total Entries : 1DES-1210-52/ME:5#
```

show mld_snooping host

Purpose	To display information of MLD snooping host on the Switch.
Syntax	**show mld_snooping host [vlan_name <string 32> | vlanid <vidlist> | all | ports <portlist> | group <ipv6_addr>]**
Description	The **show mld_snooping host** command displays information of MLD snooping host on the Switch.
Parameters	*vlan_name <string 32>* – Specifies on which VLAN mld snooping groups should be shown. *vlanid <vidlist>* – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch. *ports <portlist>* – Specifies the ports of MLD snooping host to be displayed. *group <ipv6_addr>* – Specifies the IPv6 address.
Restrictions	None.

Example usage:

To show the MLD_snooping host:

```
DES-1210-52/ME:5# show mld_snooping host vlan_name default
Command: show mld_snooping host vlan_name default



Total Entries : 0
DES-1210-52/ME:5#
```

38

LIMITED IP MULTICAST ADDRESS COMMANDS

The 802.1X commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create mcast_filter_profile	[ipv4 | ipv6] profile_id <integer 1-24> profile_name <string 20>
config mcast_filter_profile profile_id	<integer 1-24> [[add | delete] <mcast_addr> | profile_name <string 20>]
config mcast_filter_profile profile_name	<string 32> [[add | delete] <mcast_addr> | profile_name <string 20>]
config mcast_filter_profile ipv6	[profile_id <integer 1-24> | profile_name <string 20>] [add | delete] <mcastv6_addr>
delete mcast_filter_profile	[ipv4 | ipv6] [profile_id [all | <integer 1-24>] | profile_name <string 20>]
show mcast_filter_profile	{[ipv4 | ipv6]} {profile_id <integer 1-24> | profile_name <string 3220
config limited_multicast_addr	ports <portlist> [ipv4 | ipv6] {[add | delete] [profile_id <integer 1-24> | profile_name <string 20>] | access [permit | deny]}
show limited_multicast_addr	ports <portlist> {[ipv4 | ipv6]}
config max_mcast_group	ports <portlist> [ipv4 | ipv6] max_group <integer 1-512>
show max_mcast_group	ports <portlist> {[ipv4 | ipv6]}

Each command is listed in detail, as follows:

create mcast_filter_profile

Purpose	To create multicast filtering profile on the Switch.
Syntax	**create mcast_filter_profile [ipv4 | ipv6] profile_id <integer 1-24> profile_name <string 20>**
Description	The **create mcast_filter_profile** command displays the multicast filtering profiles settings.
Parameters	*[ipv4 | ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be created on the Switch. *profile_id <integer 1-24>* - Specify the profile id of multicast filter profile on the Switch. *profile_name <string 20>* - Specify the profile name of multicast filter

	profile on the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create an IPv6 multicast filtering profile on the Switch:

```
DES-1210-52/ME:5# create mcast_filter_profile ipv6 profile_id 1 profile_name
rd2
Command: create mcast_filter_profile ipv6 profile_id 1 profile_name rd2

Success.

DES-1210-52/ME:5#
```

config mcast_filter_profile profile_id

Purpose	To configure multicast filtering profile on the Switch.
Syntax	**config mcast_filter_profile profile_id <integer 1-24> [[add | delete] <mcast_addr> | profile_name <string 20>]**
Description	The **config mcast_filter_profile** command displays the multicast filtering profiles settings.
Parameters	*<integer 1-24>* - Specify the profile id to be added or deleted for the multicast filter. *[add | delete]* – Add or delete the profile id which user specified. *<mcast_addr>* – Specify the range of MAC address. *profile_name <string 20>* – Configures the profile name of the profile ID.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add the multicast address range 225.1.1.1 to 225.1.1.10 to the profile on the Switch:

```
DES-1210-52/ME:5# config mcast_filter_profile profile_id 3 add 225.1.1.1
225.1.1.10
Command: config mcast_filter_profile profile_id 3 add 225.1.1.1 225.1.1.10

Success.
DES-1210-52/ME:5#
```

config mcast_filter_profile profile_name

Purpose	To configure multicast filtering profile on the Switch.
Syntax	**config mcast_filter_profile profile_name <string 20> [[add | delete] <mcast_addr> | profile_name <string 20>]**
Description	The **config mcast_filter_profile profile_name** command displays the multicast filtering profiles settings.
Parameters	*<string 32>* - The name of the VLAN on which the MAC address resides. *[add | delete]* – Add or delete the profile id which user specified. *<mcast_addr>* – Specify the range of MAC address. *profile_name <string 20>* – Configures the profile name of the profile

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

Example usage:

To configure the multicast address range 225.1.1.1 to 225.1.1.10 to the profile name "rd3" on the Switch:

```
DES-1210-52/ME:5# config mcast_filter_profile profile_name rd3 add
225.1.1.11 225.1.1.20
Command: config mcast_filter_profile profile_name rd3 add 225.1.1.11
225.1.1.20

Success.

DES-1210-52/ME:5#
```

config mcast_filter_profile ipv6

Purpose	To configure IPv6 multicast filtering profile on the Switch.
Syntax	**config mcast_filter_profile ipv6 [profile_id <integer 1-24> | profile_name <string 20>] [add | delete] <mcastv6_addr>**
Description	The **config mcast_filter_profile ipv6** command is used to add or delete a range of IPv6 multicast addresses to the profile
Parameters	*profile_id <integer 1-24>* - Specify the profile id to be added or deleted for the multicast filter. *profile_name <string 20>* - The name of the VLAN on which the MAC address resides. *[add | delete]* – Add or delete the profile id which user specified. *<mcastv6_addr>* – Lists the IPv6 multicast addresses to put in the profile.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add the IPv6 multicast address range FFF0E::100:0:0:20 – FFF0E::100:0:0:22 to profile ID 4 on the Switch:

```
DES-1210-52/ME:5# config mcast_filter_profile ipv6 profile_id 4 add
FF0E::100:0:0:20 FF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 4 add
FF0E::100:0:0:20 FF0E::100:0:0:22

Success.
DES-1210-52/ME:5#
```

delete mcast_filter_profile

Purpose	To delete an entry in the Switch's forwarding database.
Syntax	**delete mcast_filter_profile [ipv4 | ipv6] [profile_id [all | <integer 1-24>] | profile_name <string 20>]**
Description	The **delete mcast_filter_profile** command deletes a profile in the Switch's multicast forwarding filtering database.
Parameters	*[ipv4 | ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be removed on the Switch.

	profile_id [all | *<integer 1-24>]* − The profile id of the VLAN on which the multicast forwarding filtering database resides. *profile_name <string 20>* − The name of the VLAN on which the multicast forwarding filtering database resides.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete the IPv4 multicast address profile with a profile name of rd3:

```
DES-1210-52/ME:5# delete mcast_filter_profile ipv4 profile_name rd3
Command: delete mcast_filter_profile ipv4 profile_name rd3

Success.
DES-1210-52/ME:5#
```

show mcast_filter_profile

Purpose	To display multicast filtering settings on the Switch.
Syntax	**show mcast_filter_profile {[ipv4 | ipv6]} {profile_id <integer 1-24> | profile_name <string 20>}**
Description	The **show mcast_filter_profile** command displays the multicast filtering profiles settings.
Parameters	*[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be displayed on the Switch. *profile_id <integer 1-24>* - Specify the profile id of multicast filter profile to be displayed. *profile_name <string 20>* - Specify the profile name of multicast filter profile to be displayed.
Restrictions	None.

Example usage:

To display all the defined multicast address profiles:

```
DES-1210-52/ME:5# show mcast_filter_profile
Command: show mcast_filter_profile

Type  Profile ID Profile Name
-----  ------------  -------------------------------
v6     1             rd2
v6     4             rd4

[v6 Profiles]
ID   IPv6 Address Range
--   ----------------------------------------
4    ff0e:0000:0000:0000:0100:0000:0000:0020 ~
     ff0e:0000:0000:0000:0100:0000:0000:0022

DES-1210-52/ME:5#
```

config limited_multicast_addr

Purpose	To configure the multicast address filtering function a port.
Syntax	**config limited_multicast_addr ports <portlist> [ipv4 | ipv6] {[add | delete] [profile_id <integer 1-24> | profile_name <string 20>] | access [permit | deny]}**
Description	The **config limited_multicast_addr** command is 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	*ports <portlist>* – A port or range of port on which the limited multicast address range to be configured has been assigned. *[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be configured. *[add* | *delete]* – Add or delete a multicast address profile to a port. *profile_id <integer 1-24>* – A profile ID to be added or deleted from a port. *profile_name <string 20>* – A profile name to be added or deleted from a port. *[permit* | *deny]* – Specifies that the packet that matches the addresses defined in the profiles will be permitted or denied. The default mode is permit.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure ports 1 and 3 to set the IPv6 multicast address profile id 1:

```
DES-1210-52/ME:5# config limited_multicast_addr ports 1,3 ipv6 add profile_id 1
Command: config limited_multicast_addr ports 1,3 ipv6 add profile_id 1

Success.
DES-1210-52/ME:5#
```

show limited_multicast_addr

Purpose	Used to show the per-port Limited IP multicast address range.
Syntax	**show limited_multicast_addr ports <portlist> {[ipv4 | ipv6]}**
Description	The **show limited_multicast_addr** command is to display the multicast address range by port or by VLAN.
Parameters	*<portlist>* – Used to show the per-port Limited IP multicast address range. *[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of limited multicast address to be displayed.
Restrictions	None.

Example usage:

To show the IPv4 limited multicast address on ports 1 and 3:

```
DES-1210-52/ME:5# show limited_multicast_addr ports 1,3 ipv4
Command: show limited_multicast_addr ports 1,3 ipv4

Port Access     Profile ID List
----  ----------     -----------------------------------------------------------
```

```
1      (v4) Permit
3      (v4) Permit

DES-1210-52/ME:5#
```

config max_mcast_group

Purpose	Used to configure the maximum number of multicast groups that a port can join.
Syntax	**config max_mcast_group ports <portlist> [ipv4 | ipv6] max_group <integer 1-512>**
Description	The **config max_mcast_group** command is used to configure the maximum number of multicast groups that a port can join.
Parameters	*<portlist>* – A range of ports to configure the maximum multicast group. *[ipv4 | ipv6]* – Specify the IPv4 or IPv6 to be configured. *max_group <integer 1-512>* – Specifies the maximum number of multicast groups. The range is from 1 to 512.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the IPv4 maximum multicast address groups on ports 1 and 3 as 100:

```
DES-1210-52/ME:5# config max_mcast_group ports 1,3 ipv4 max_group 100
Command: config max_mcast_group ports 1,3 ipv4 max_group 100

Success.

DES-1210-52/ME:5#
```

show max_mcast_group

Purpose	To display maximum multicast group ports on the Switch.
Syntax	**show max_mcast_group ports <portlist> {[ipv4 | ipv6]}**
Description	The **show max_mcast_group** command displays the multicast filtering profiles settings.
Parameters	*<portlist>* - Specify a port or range of ports to be displayed. *{[ipv4 | ipv6]}* – Specify the IPv4 or IPv6 to be displayed.
Restrictions	None.

Example usage:

To show IPv6 maximum multicast group port 1 and 3 settings:

```
DES-1210-52/ME:5# show max_mcast_group ports 1,3 ipv6
Command: show max_mcast_group ports 1,3 ipv6

Port Max Group
----- --------------------
1      (v6) 256
3      (v6) 256
```

```
DES-1210-52/ME:5#
```

39

LAYER 2 PROTOCOL TUNNELING COMMANDS

The Layer 2 Protocol Tunneling (L2PT) Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable l2protocol_tunnel	
disable l2protocol_tunnel	
config l2protocol_tunnel ports	[all | <portlist>] type [uni tunneled_protocol {[stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD] | all]} | nni | none] {threshold <value 0-65535>}
show l2protocol_tunnel	{[nni | uni]}

Each command is listed in detail, as follows:

enable l2protocol_tunnel

Purpose	To enable the Layer 2 protocol tunneling function.
Syntax	**enable l2protocol_tunnel**
Description	The **enable l2protocol_tunnel** command is used to enable the Layer 2 protocol tunneling function on the Switch.
Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To enable Layer 2 protocol tunnel of the Switch:

```
DES-1210-52/ME:5# enable l2protocol_tunnel
Command: enable l2protocol_tunnel


Success.
DES-1210-52/ME:5#
```

disable l2protocol_tunnel

Purpose	To disable the Layer 2 protocol tunneling function.
Syntax	**disable l2protocol_tunnel**
Description	The **disable l2protocol_tunnel** command is used to disable the Layer 2 protocol tunneling function on the Switch.
Parameters	None.

Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To disable Layer 2 protocol tunnel of the Switch:

```
DES-1210-52/ME:5# disable l2protocol_tunnel
Command: disable l2protocol_tunnel


Success.
DES-1210-52/ME:5#
```

config l2protocol_tunnel

Purpose	To configure Layer 2 protocol tunneling on ports.
Syntax	**config l2protocol_tunnel ports [all | <portlist>] type [uni tunneled_protocol {[stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD] | all]} | nni | none] {threshold <value 0-65535>}**
Description	The **show l2protocol_tunnel** command is used to configure Layer 2 protocol tunneling on ports on the Switch.
Parameters	*[all | <portlist>]* – Specify a list of ports or all ports on which the Layer 2 protocol tunneling to be configured. *uni* - Specify the ports as UNI ports 2. *tunneled_protocol* - Specify tunneled protocols on the UNI ports. STP –Specify to use the STP protocol Gvrp –Specify to use the GVRP protocol *protocol_mac* - Specify the destination MAC address of the L2 protocol packets that will tunneled on these UNI ports. nni - Specify the ports as NNI ports *threshold <value 0-65535>* - Specify the drop threshold for packets-per-second accepted on theUNI ports. The ports drop the PDU if the protocol's threshold is exceeded.
Restrictions	None.

Example usage:

To configure Layer 2 protocol tunnel of the Switch:

```
DES-1210-52/ME:5# config l2protocol_tunnel ports 6-8 type nni
Command: config l2protocol_tunnel ports 6-8 type nni


Success.
DES-1210-52/ME:5#
```

show l2protocol_tunnel

Purpose	To display the Layer 2 protocol tunneling function.
Syntax	**show l2protocol_tunnel {[nni | uni]}**
Description	The **show l2protocol_tunnel** command is used to display the Layer

	2 protocol tunneling function on the Switch.
Parameters	*nni* – Specify to show UNI detail information, include tunneled and dropped PDU statistic. *uni* - Specify to show NNI detail information, include de-capsulated Layer 2 PDU PDU statistic.
Restrictions	None.

Example usage:

To display Layer 2 protocol tunnel of the Switch:

```
DES-1210-52/ME:5# show l2protocol_tunnel
Command: show l2protocol_tunnel


Global State : Enabled
UNI Ports      :
NNI Ports      :

Success.
DES-1210-52/ME:5#
```

40

802.1X COMMANDS

The 802.1X commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable 802.1x	
disable 802.1x	
show 802.1x auth_state	{ports <portlist>}
show 802.1x auth_configuration	{ports <portlist>}
config 802.1x auth_parameter ports	[<portlist> | all] [default | { 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] | direction [both | in]}]
config 802.1x init	port_based ports [<portlist> | all]
config 802.1x auth_protocol	[radius_eap | local]
config 802.1x reauth	port_based ports [<portlist> | all]
config radius add	<server_index 1-3> [<ipaddr> | <ipv6_addr>] [key <passwd 32>] {default | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | retransmit <int 1-255> | timeout <int 1-255>}
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> { key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | ipaddress [<ipaddr> | <ipv6_addr>] | retransmit <int 1-255> | timeout <int 1-255>}
show radius	
config 802.1x fwd_pdu system	[enable | disable]
show 802.1x fwd_pdu system status	
config 802.1x auth_mode	[port_based | mac_based]
create 802.1x guest vlan	<vlan_name 32>
delete 802.1x guest vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> | all] state [enable | disable]
show 802.1x	

Command	Parameter
guest_vlan	
create 802.1x user	<username 15>
show 802.1x user	
delete 802.1x user	<username 15>
config 802.1x capability ports	[<portlist> | all] [authenticator | none]

Each command is listed in detail, as follows:

enable 802.1x

Purpose	To enable the 802.1x server on the Switch.
Syntax	**enable 802.1x**
Description	The **enable 802.1x** command enables the 802.1x Port-based Network Access control server application on the Switch.
Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To enable 802.1x switch wide:

```
DES-1210-52/ME:5# enable 802.1x
Command: enable 802.1x


Success.
DES-1210-52/ME:5#
```

disable 802.1x

Purpose	To disable the 802.1x server on the Switch.
Syntax	**disable 802.1x**
Description	The **disable 802.1x** command disables the 802.1x Port-based Network Access control server application on the Switch.
Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To disable 802.1x on the Switch:

```
DES-1210-52/ME:5# disable 802.1x
Command: disable 802.1x
```

```
Success.
DES-1210-52/ME:5#
```

show 802.1x

Purpose	To display the 802.1x server information on the Switch.
Syntax	**show 802.1x**
Description	The **show 802.1x** command displays the 802.1x Port-based Network Access control server application on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display 802.1x on the Switch:

```
DES-1210-52/ME:5# show 802.1x
Command: show 802.1x

802.1X                    : Enable
Authentication Mode       : Port_base
Authentication Method     : Local

Success.
DES-1210-52/ME:5#
```

show 802.1x auth_state

Purpose	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 displays the current 802.1x authentication state of the specified ports of the Port-based Network Access Control server application on the Switch. The following details are 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.
Parameters	*ports <portlist>* − A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the 802.1x authentication states for port 1~5 (stacking disabled) for Port-based 802.1x:

```
DES-1210-52/ME:5# show 802.1x auth_state ports 1-5
Command: show 802.1x auth_state ports 1-5

Port   Auth PAE State  Backend State   Port Status
------ --------------- --------------- ---------------
1      ForceAuth       Success.         Authorized
2      ForceAuth       Success.         Authorized
3      ForceAuth       Success.         Authorized
4      ForceAuth       Success.         Authorized
5      ForceAuth       Success.         Authorized
DES-1210-52/ME:5#
```

show 802.1x auth_configuration

Purpose	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 auth_configuration** command displays the current configuration of the 802.1x Port-based Network Access Control server application on the Switch. The following details are displayed: *802.1x:* Enabled/Disabled − Shows the current status of 802.1x functions on the Switch. *Authentication Mode:* Port-based/Mac-based/None − Shows the 802.1x authorization mode. Authentication Method: Remote/none − Shows the type of authentication protocol suite in use between the Switch and a RADIUS server. *Port number :* Shows the physical port number on the Switch. *AdminCrlDir:* 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. *OpenCrlDir:* 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 Success.ive

	reauthentications. *ReAuthenticate:* true/false − Shows whether or not to reauthenticate.
Parameters	*ports <portlist>* − Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display the 802.1x configurations of port 2:

```
DES-1210-52/ME:5# show 802.1x auth_configuration ports 2
Command: show 802.1x auth_configuration ports 2

Authentication Mode     : Port_base

Port number    : 1
Capability     : none
AdminCrlDir    : Both
OpenCrlDir     : Both
Port Control   : ForceAuthorized
QuietPeriod    : 60    sec
TxPeriod       : 30    sec
SuppTimeout    : 30    sec
ServerTimeout  : 30    sec
MaxReq         : 2     times
ReAuthPeriod   : 3600  sec
ReAuthenticate : Disable

Port number    : 2
Capability     : none
AdminCrlDir    : Both
OpenCrlDir     : Both
Port Control   : ForceAuthorized
QuietPeriod    : 60    sec
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

config 802.1x auth_parameter ports

Purpose	To configure the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.
Syntax	**config 802.1x auth_parameter ports [<portlist> | all] [default | { 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] | direction [both | in]}]**
Description	The **config 802.1x auth_parameter ports** command configures the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.
Parameters	*[<portlist>* | *all]* – A port, range of ports or all 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. *port_control* – Configures the administrative control over the authentication process for the range of ports. The options are: • *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 is 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>* - Configures 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 300-4294967295>* – Configures the time interval between Success.ive 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. *direction [both | in]* –Sets the administrative-controlled direction to *Both*. If *Both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. The *In* option is not supported in the present firmware release.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

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

```
DES-1210-52/ME:5# config 802.1x auth_parameter ports 1-5 direction both
Command: config 802.1x auth_parameter ports 1-5 direction both



Success.
DES-1210-52/ME:5#
```

config 802.1x init

Purpose	To initialize the 802.1x function on a range of ports.
Syntax	**config 802.1x init port_based ports [<portlist> | all]**
Description	The **config 802.1x init** command initializes 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* – Instructs the Switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified. *ports <portlist>* – A port or range of ports to be configured. *all* – Specifies all of the ports on the Switch.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To initialize the authentication state machine of all ports:

```
DES-1210-52/ME:5# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-1210-52/ME:5#
```

config 802.1x auth_protocol

Purpose	To configure the 802.1x authentication protocol on the Switch .
Syntax	**config 802.1x auth_protocol [radius_eap | local]**
Description	The **config 802.1x auth_protocol** command enables configuration of the authentication protocol.
Parameters	*radius_eap* – Uses the list of RADIUS EAP servers for authentication. *local* – Uses no authentication.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure the RADIUS (AAA) authentication protocol on the Switch:

```
DES-1210-52/ME:5# config 802.1x auth_protocol local
Command: config 802.1x auth_protocol local

Success.

DES-1210-52/ME:5#
```

config 802.1x reauth

Purpose	To configure the 802.1x re-authentication feature of the Switch.
Syntax	**config 802.1x reauth port_based ports [<portlist> | all]**
Description	The **config 802.1x reauth** command re-authenticates a previously authenticated device based on port number.
Parameters	*port_based* – Instructs the Switch to re-authorize 802.1x functions based only on the port number. Ports approved for re-authorization can then be specified.

	ports <portlist> – A port or range of ports to be re-authorized. *all* – Specifies all of the ports on the Switch.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-18:

```
DES-1210-52/ME:5# config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-1210-52/ME:5#
```

config radius add

Purpose	To configure the settings the Switch uses to communicate with a RADIUS server.
Syntax	**config radius add <server_index 1-3> [<ipaddr> | <ipv6_addr>] [key <passwd 32>] {default | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | retransmit <int 1-255> | timeout <int 1-255>}**
Description	The **config radius add** command configures the settings the Switch uses to communicate with a RADIUS server.
Parameters	*<server_index 1-3>* – The index of the RADIUS server. *[<ipaddr>* | *<ipv6_addr]>* – The IPv4 or IPv6 address of the RADIUS server. *key* – Specifies that a password and encryption key are to 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 128 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. *retransmit <int 1-255>* – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. *timeout <int 1-255>* – Specifies the connection timeout. The value may be between 1 and 255 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DES-1210-52/ME:5# config radius add 1 10.48.47.11 key dlink default
Command: config radius add 1 10.48.47.11 key dlink default
```

```
Success.
DES-1210-52/ME:5#
```

config radius delete	
Purpose	To delete a previously entered RADIUS server configuration.
Syntax	**config radius delete <server_index 1-3>**
Description	The **config radius delete** command deletes a previously entered RADIUS server configuration.
Parameters	*<server_index 1-3>* – The index of the RADIUS server.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DES-1210-52/ME:5# config radius delete 1
Command: config radius delete 1

Success.
DES-1210-52/ME:5# #
```

config radius	
Purpose	To configure the Switch's RADIUS settings.
Syntax	**config radius <server_index 1-3> { key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | ipaddress [<ipaddr> | <ipv6_addr>] | retransmit <int 1-255> | timeout <int 1-255>}**
Description	The **config radius** command configures the Switch's RADIUS settings.
Parameters	*<server_index 1-3>* – The index of the RADIUS server. *key* – Specifies that a password and encryption key are to 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. *ipaddress [<ipaddr>* | *<ipv6_addr>]* – The IPv4 or IPv6 address of the RADIUS server. *retransmit <int 1-255>* – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. *timeout <int 1-255>* – Specifies the connection timeout. The value may be between 1 and 255 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DES-1210-52/ME:5# config radius 1 ipaddress 10.48.47.11
Command: config radius 1 ipaddress 10.48.47.11



Success.
DES-1210-52/ME:5#
```

show radius

Purpose	To display the current RADIUS configurations on the Switch.
Syntax	**show radius**
Description	The **show radius** command displays the current RADIUS configurations on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display RADIUS settings on the Switch:

```
DES-1210-52/ME:5# show radius
Command: show radius

Index  Ip Address      Auth-Port  Acct-Port  Timeout  Retransmit  Key
                                             (secs)
-----  ----------------  ---------  ----------  ---------  ---------------  ------
1      10.48.74.121    1812       1813       5        10          dlink

Total Entries : 1


Success.
DES-1210-52/ME:5#
```

config 802.1x fwd_pdu system

Purpose	To configure the 802.1x forwarding EAPOL PDU on the Switch.
Syntax	**config 802.1x fwd_pdu system [enable | disable]**
Description	The **config 802.1x fwd_pdu system** command is used to configure the control of forwarding EAPOL PDUs. Then the 802.1x functionality is disabled, for a port, and if the 802.1x forwarding PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded on the same VLAN to those ports of which the 802.1x forwarding PDU is enabled and 802.1x is disabled (globally or just for the port)
Parameters	*[enable* | *disable]* – Specifies the forwarding of EAPOL PDU is enabled or disabled. The default is disabled.
Restrictions	Only Administrator, operator or power user-level users can issue this

	command.

Example usage:

To enable 802.1x forwarding EAPOL PDU

```
DES-1210-52/ME:5# config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable



Success.
DES-1210-52/ME:5#
```

show 802.1x fwd_pdu system status

Purpose	To display the 802.1x forwarding EAPOL PDU status on the Switch.
Syntax	**show 802.1x fwd_pdu system status**
Description	The **show 802.1x fwd_pdu system status** command is used to display the control of forwarding EAPOL PDUs.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1x forwarding EAPOL PDU status:

```
DES-1210-52/ME:5# show 802.1x fwd_pdu system status
Command: show 802.1x fwd_pdu system status

PNAC control packet (eap) is forwarding....

Success.
DES-1210-52/ME:5#
```

config 802.1x auth_mode

Purpose	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 auth_mode** command enables either the port-based or MAC-based 802.1x authentication feature on the Switch.
Parameters	*[port_based* | *mac_based]* – Specifies whether 802.1x authentication is by port or MAC address.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure 802.1x authentication by port address:

```
DES-1210-52/ME:5# config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based



Success.
DES-1210-52/ME:5#
```

create 802.1x guest_vlan

Purpose	Enables network access to a Guest VLAN.
Syntax	**create 802.1x guest_vlan <vlan_name 32>**
Description	The **create 802.1x guest_vlan** command enables network access to a 802.1x Guest VLAN. A network administrator can use 802.1x Guest VLANs to deny network access via port–based authentication, but grant Internet access to unauthorized users.
Parameters	<*vlan_name 32*> **−** The name of the 802.1x Guest VLAN to be created.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a 802.1x Guest VLAN:

```
DES-1210-52/ME:5# create 802.1x guest_vlan default
Command: create 802.1x guest_vlan default

Success.

DES-1210-52/ME:5#
```

delete 802.1x guest_vlan

Purpose	Disables network access to a Guest VLAN.
Syntax	**delete 802.1x guest_vlan <vlan_name 32>**
Description	The **delete 802.1x guest_vlan** command disables network access to a 802.1x Guest VLAN. A network administrator can use 802.1x Guest VLANs to deny network access via port–based authentication, but grant Internet access to unauthorized users.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command. The user is required to disable Guest VLAN before deleting a specific the VLAN.

Example usage:

To delete a 802.1x Guest VLAN

```
DES-1210-52/ME:5# delete 802.1x guest_vlan default
Command: delete 802.1x guest_vlan default

Success.

DES-1210-52/ME:5#
```

config 802.1x guest_vlan ports

Purpose	Defines a port or range of ports to be members of the Guest VLAN.
Syntax	**config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]**
Description	The **config 802.1x guest_vlan ports** command defines a port or range of ports to be members of the 802.1x Guest VLAN. The 802.1x Guest VLAN can be be configured to provide limited network access to authorized member ports. If a member port is denied network access via port–based authorization, but the 802.1x Guest VLAN is enabled, the member port receives limited network access. For example, a network administrator can use the 802.1x Guest VLAN to deny internal network access via port–based authentication, but grant Internet access to unauthorized users.
Parameters	*<portlist>* – A port or range of ports to be configured to the Guest VLAN. *All* – Indicates all ports to be configured to the guest vlan. *state [enable* | *disable]* – Specifies the guest vlan port is enabled or disabled of the switch.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure ports to the Guest VLAN

```
DES-1210-52/ME:5# config 802.1x guest_vlan ports 1-5 state enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DES-1210-52/ME:5#
```

show 802.1x guest_vlan

Purpose	Displays configuration information for the Guest VLAN.
Syntax	**show 802.1x guest_vlan**
Description	The **show 802.1x guest_vlan** command displays the Guest VLAN name, state, and member ports.
Parameters	None.
Restrictions	None.

Example usage:

To display the Guest VLAN configuration information:

```
DES-1210-52/ME:5# show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Settings
-----------------------------------------------------------------------
Guest VLAN                          : default
Enabled Guest VLAN Ports :
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,2
1,22,23,24,25,26,27,28

DES-1210-52/ME:5#
```

create 802.1x user

Purpose	Enable network access to a 802.1x user.
Syntax	**create 802.1x user <username 15>**
Description	The **create 802.1x user** command enables network access to a 802.1x user.
Parameters	*<vlan_name 15>* − The name of the 802.1x user to be created.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To create a 802.1x user:

```
DES-1210-52/ME:5# create 802.1x user dlink
Command: create 802.1x user dlink

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

Success.
DES-1210-52/ME:5#
```

show 802.1x user

Purpose	Displays the user information for the Guest VLAN.
Syntax	**show 802.1x user**
Description	The **show 802.1x user** command displays the 802.1x user information on the Switch.
Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To display the 802.1x user information:

```
DES-1210-52/ME:5# show 802.1x user
Command: show 802.1x user

Index       Username
------------   ---------------
  1           dlink

Total Entries: 1

Success.
DES-1210-52/ME:5#
```

delete 802.1x user

Purpose	Deletes network access to a 802.1x user.
Syntax	**delete 802.1x user <username 15>**
Description	The **delete 802.1x user** command deletes network access to a 802.1x user.
Parameters	*<username 15>* − The name of the 802.1x user to be deleted.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To delete the 802.1x user:

```
DES-1210-52/ME:5# delete 802.1x user dlink
Command: delete 802.1x user dlink



Success.
DES-1210-52/ME:5#
```

config 802.1x capability ports

Purpose	Defines a port or range of ports to be members of the Guest VLAN.
Syntax	**config 802.1x capability ports [<portlist> | all] [authenticator | none]**
Description	Th **config 802.1x capability ports** is used to configure the capability for the 802.1x on the Switch.
Parameters	*<portlist>* – A port or range of ports to be configured to the 802.1x capability. *all* – Indicates all ports to be configured to the 802.1x capability. *[authenticator | none]* – Specifies the 802.1x capability port to be authenticator or none.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure capability ports to the 802.1x on the Switch:

```
DES-1210-52/ME:5# config 802.1x capability ports all authenticator
Command: config 802.1x capability ports all authenticator


Success.
DES-1210-52/ME:5#
```

41

PORT SECURITY COMMANDS

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

Command	Parameter
config port_security	[<portlist> | all] [admin_state [enable | disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]
show port_security	{ports <portlist>}
delete port_security_entry	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>

Each command is listed in detail, as follows:

config port_security

Purpose	To configure port security settings.
Syntax	**config port_security [<portlist> | all] [admin_state [enable | disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]**
Description	The **config port_security** command configures port security settings for specific ports.
Parameters	*<portlist>* – A port or range of ports to be configured. *all* – Configures port security for all ports on the Switch. *admin_state [enable | disable]* – Enables or disables port security for the listed ports. *max_learning_addr <int 0-64>* - Specify the max learning address. The range is 0 to 64. 1-64 Limits the number of MAC addresses dynamically listed in the FDB for the ports. *lock_address_mode – Defines the TBD and contains the following options:* • *Permenant – Learns up to the maximum number of dynamic addresses allowed on the port. The learned addresses are not aged out or relearned on other port for as long as the port is locked.* • *DeleteOnReset – Deletes the current dynamic MAC addresses associated with the port. Learn up to the maximum addresses allowed on the port (this number is also configurable). Aging is disabled; the addresses are deleted on reset* • *DeleteOnTimeout – Deletes the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Re-learned MAC addresses and address aging out are also enabled. The MAC addresses are deleted when the device is reset*

	and on when the address is aged out.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To configure port security:

```
DES-1210-52/ME:5# config port_security 1-5 admin_state enable max_learning_addr 5 lock_address_mode DeleteOnReset
Command: config port_security 1-5 admin_state enable max_learning_addr 5 lock_address_mode DeleteOnReset



Success.
DES-1210-52/ME:5#
```

show port_security

Purpose	To display the current port security configuration.
Syntax	**show port_security {ports <portlist>}**
Description	The **show port_security** command displays port security information for the Switch's ports. The information displayed includes port security, admin state, maximum number of learning address and lock mode and trap interval.
Parameters	*ports <portlist>* – A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DES-1210-52/ME:5# show port_security ports 1-5
Command: show port_security ports 1-5



Port  Admin state Max.Learning Addr. Lock Address Mode
----    -------------      -------------------------    -------------------
1      enabled        5                          DeleteOnReset
2      enabled        5                          DeleteOnReset
3      enabled        5                          DeleteOnReset
4      enabled        5                          DeleteOnReset
5      enabled        5                          DeleteOnReset

DES-1210-52/ME:5#
```

delete port_security _entry

Purpose	To delete a port security entry by VLAN, VLAN ID, and MAC address.
Syntax	**delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>**
Description	The **delete port_security_entry** command is used to delete a port security entry by VLAN, VLAN ID, and MAC address.
Parameters	<*vlan_name 32*> – Specifies the VLAN name. <*vlanid 1-4094*> - Specifies the VLAN ID. <*macaddr*> - Specifies the MAC address.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To delete the port security entry with a MAC address of 00-01-30-10-2c-c7 on the default VLAN:

```
DES-1210-52/ME:5# delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7
Command: delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7


Success.
DES-1210-52/ME:5#
```

42

TIME AND SNTP COMMANDS

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

Command	Parameter
config sntp	{primary [<ipaddr> | <ipv6addr>] | secondary [<ipaddr> | <ipv6addr>] | poll-interval <sec 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	<date> <systime>
config time_zone operator	[+ hour <gmt_hour 0-13> minute <minute 0-59> | - hour <gmt_hour 0-12> minute <minute 0-59>]
config dst	[disable | [annual s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time> end_date <int 1-31> e_mth <end_mth 1-12> e_time <end_time> | offset [30 | 60 | 90 | 120]]]
show time	

Each command is listed in detail, as follows:

config sntp	
Purpose	To setup SNTP service.
Syntax	**config sntp {primary [<ipaddr> | <ipv6addr>] | secondary [<ipaddr> | <ipv6addr>] | poll-interval <sec 30-99999>}**
Description	The **config sntp** command configures SNTP service from an SNTP server. SNTP must be enabled for this command to function (See **enable sntp**).
Parameters	*primary [<ipaddr>*| *<ipv6addr>]* – Specifies the IPv4 or IPv6 address of the primary SNTP server. *secondary [<ipaddr>*| *<ipv6addr>]* – Specifies the IPv4 or IPv6 address of the secondary SNTP server. *poll-interval <sec 30-99999>* – The interval between requests for updated SNTP information. The polling interval ranges from 60 seconds (1 minute) to 86,400 seconds (1 day).
Restrictions	Only administrator or operate-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-1210-52/ME:5# config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 60
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 60

Success.

DES-1210-52/ME:5#
```

show sntp

Purpose	To display the SNTP information.
Syntax	**show sntp**
Description	The **show sntp** command displays SNTP settings information, including the source IP address, time source and poll interval.
Parameters	None.
Restrictions	None.

Example usage:

To display SNTP configuration information:

```
DES-1210-52/ME:5# show sntp
Command: show sntp


SNTP Information
-----------------------------------------
Current Time Source          : Local
SNTP                         : Disabled
SNTP Primary Server          : 10.1.1.1
SNTP Secondary Server        : 10.1.1.2
SNTP Poll Interval           : 60 sec

DES-1210-52/ME:5#
```

enable sntp

Purpose	To enable SNTP server support.
Syntax	**enable sntp**
Description	The **enable sntp** command enables SNTP server support. SNTP service must be separately configured (see **config sntp**). Enabling and configuring SNTP support override any manually configured system time settings.
Parameters	None.
Restrictions	Only administrator and 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-1210-52/ME:5# enable sntp
Command: enable sntp


Success.

DES-1210-52/ME:5#
```

disable sntp

Purpose	To disable SNTP server support.
Syntax	**disable sntp**
Description	The **disable sntp** command disables SNTP support.
Parameters	None.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To disable SNTP support:

```
DES-1210-52/ME:5# disable sntp
Command: disable sntp

Success.

DES-1210-52/ME:5#
```

config time

Purpose	To manually configure system time and date settings.
Syntax	**config time <date> <systime>**
Description	The **config time date** command configures the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	*<date>* –Specifies the date, using two numerical characters for the day of the month, English abbreviation for the name of the month, and four numerical characters for the year. For example: 19jan2011. *<systime >* – Specifies 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 operate-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-1210-52/ME:5# config time 09jan2012 15:50:50
Command: config time 09jan2012 15:50:50

Success.

DES-1210-52/ME:5#
```

config time_zone operator

Purpose	To determine the time zone used in order to adjust the system clock.
Syntax	**config time_zone operator [+ hour <gmt_hour 0-13> minute <minute 0-59> | - hour <gmt_hour 0-12> minute <minute 0-59>]**
Description	The **config time_zone operator** command adjusts the system clock settings according to the time zone. Time zone settings adjust SNTP information accordingly.
Parameters	*operator* – May be (+) to add or (-) to subtract time to adjust for time zone relative to GMT. *hour <gmt_hour 0-13>* – Specifies the number of hours difference from GMT. *Minute <minute 0-59>* – Specifies the number of minutes 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-1210-52/ME:5# config time_zone operator + hour 2 minute 30
Command: config time_zone operator + hour 2 minute 30

Success.

DES-1210-52/ME:5#
```

config dst

Purpose	To configure time adjustments to allow for the use of Daylight Saving Time (DST).
Syntax	**config dst [disable | [annual s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time> end_date <int 1-31> e_mth <end_mth 1-12> e_time <end_time> | offset [30 | 60 | 90 | 120]]]**
Description	The **config dst** command disables or configures Daylight Saving Time (DST). When enabled, this adjusts the system clock to comply with any DST requirement. DST adjustment affects system time for both manually configured time and time set using SNTP service.
Parameters	*disable* – Disables the DST seasonal time adjustment for the Switch. *annual* – Enables DST seasonal time adjustment on an annual basis. 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. The format for annual mode is as follows, and in the order listed:

	• *s_date <start_date 1-31>* - The day of the month to begin DST, expressed numerically**.** • *s_mth <start_mth 1-12>* - The month of the year to begin DST, expressed numerically. • *s_time <start_time>* - The time of day to begin DST in hours and minutes, expressed using a 24-hour clock. • *end_date <int 1-31>* - The day of the month to end DST, expressed numerically**.** • *e_mth <end_mth 1-12>* - The month of the year to end DST, expressed numerically. • *e_time<end_time>* - The time of day to end DST, in hours and minutes, expressed using a 24-hour clock. *offset [30* | *60* | *90* | *120]* – Indicates the number of minutes to add during the summertime. The possible offset times are 30, 60, 90, and 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 to run from the 2nd Tuesday in April at 3 PM until the 2nd Wednesday in October at 3:30 PM and add 30 minutes at the onset of DST:

```
DES-1210-52/ME:5# config dst annual s_date 2 s_mth 4 s_time 3 end_date 2
e_mth 10 e_time 3 offset 30
Command: config dst annual s_date 2 s_mth 4 s_time 3 end_date 2 e_mth 10
e_time 3 offset 30



Success.

DES-1210-52/ME:5#
```

show time

Purpose	To display the current time settings and status.
Syntax	**show time**
Description	The **show time** command displays the system time and date configuration, as well as displays the current system time.
Parameters	None.
Restrictions	None.

Example usage:

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

```
DES-1210-52/ME:5# show time
Command: show time

Time information
-------------------------------------------------------------------------------------------
Current Time Source                   : Local
Current Time                          : 09 Jan 2012 15:56:02
GMT Time Zone offset                  : GMT +02:30
Daylight Saving Time Status           : Disabled
Offset in Minutes                     : 60
Annual From                           : 01 Jan 00:00
To                                    : 01 Jan 00:00


DES-1210-52/ME:5#
```

43

ARP COMMANDS

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

Command	Parameter
create ArpSpoofing	ip_address <ipaddr> mac_address <macaddr> [<portlist> | all]
show ArpSpoofing	
delete ArpSpoofing	ip_address <ipaddr>
config arp_aging time	<value 0-65535 >
clear arptable	
create arpentry	<ipaddr> <macaddr>
config arpentry	<ipaddr> <macaddr>
delete arpentry	[<ipaddr> | all]
show arpentry	{information | interface_name {system} | ip_address <ipaddr> | mac_address <macaddr> | summary}
show arpentry aging_time	

Each command is listed in detail, as follows:

create ArpSpoofing

Purpose	To create the on the Switch.
Syntax	**create ArpSpoofing ip_address <ipaddr> mac_address <macaddr> [<portlist> | all]**
Description	The **create ArpSpoofing** 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	*ip_address <ipaddr>* − Specifies the IP address of the end node or station. *mac_address<macaddr>* − Specifies the MAC address corresponding to the IP address above. *[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be configured for the ARP snooping.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an ARP Spoofing IP address on the Switch:

```
DES-1210-52/ME:5# create ArpSpoofing ip_address 10.2.1.1
mac_address 00-00-00-01-01-2 all
Command: create ArpSpoofing ip_address 10.2.1.1 mac_address 00-
00-00-01-01-2 all

Success.
DES-1210-52/ME:5#
```

show ArpSpoofing

Purpose	To display the ARP Spoofing information on the Switch.
Syntax	**show ArpSpoofing**
Description	The **show ArpSpoofing** displays the information, indludes IP address, MAC address and Port list information on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the ARP Spoofing information on the Switch:

```
DES-1210-52/ME:5# show ArpSpoofing
Command: show ArpSpoofing

IP Address           MAC Address           PortList
10.2.1.1              00:00:00:01:01:02      1-52


DES-1210-52/ME:5# show ArpSpoofing
```

delete ArpSpoofing

Purpose	To delete an IP address and the corresponding MAC address into the Switch's ARP table.
Syntax	**delete ArpSpoofing ip_address <ipaddr>**
Description	The **delete ArpSpoofing** command deletes an IP address and the corresponding MAC address into the Switch's ARP table.
Parameters	*ip_address <ipaddr>* – The IP address of the end node or station.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the ARP spoofing configuration:

```
DES-1210-52/ME:5# create ArpSpoofing ip_address 10.2.1.1
mac_address 00-00-00-01-01-2 all
Command: create ArpSpoofing ip_address 10.2.1.1 mac_address 00-
00-00-01-01-2 all

Success.
DES-1210-52/ME:5#
```

config arp_aging time

Purpose	To configure the age-out timer for ARP table entries on the Switch.
Syntax	**config arp_aging time <value 0-65535>**
Description	The **config arp_aging time** 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	<*value 0-65535*> – The ARP age-out time, in minutes. The value may be 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-1210-52/ME:5# config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-1210-52/ME:5#
```

clear arptable

Purpose	To remove all dynamic ARP table entries.
Syntax	**clear arptable**
Description	The **clear arptable** 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-1210-52/ME:5# clear arptable
Command: clear arptable

Success.

DES-1210-52/ME:5#
```

create arpentry

Purpose	To create an entry for ARP table on the Switch.
Syntax	**create arpentry <ipaddr> <macaddr>**
Description	The **create arpentry <ipaddr> <macaddr>** command is used to create an entry for ARP table on the Switch.
Parameters	*<ipaddr>* – Specify the IP address to be configured. *<macaddr>* – Specify the MAC address to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create an ARP entry:

```
DES-1210-52/ME:5# create arpentry 10.90.90.94 00-00-00-01-02-03
Command: create arpentry 10.90.90.94 00-00-00-01-02-03


Success.

DES-1210-52/ME:5#
```

config arpentry

Purpose	To configure the entry for ARP table on the Switch.
Syntax	**config arpentry <ipaddr> <macaddr>**
Description	The **config arpentry** command is used to configure the entry for ARP table on the Switch.
Parameters	*<ipaddr>* – Specify the IP address to be configured. *<macaddr>* – Specify the MAC address to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure ARP entry:

```
DES-1210-52/ME:5# config arpentry 10.90.90.94 00-00-00-01-02-05
Command: config arpentry 10.90.90.94 00-00-00-01-02-05


Success.

DES-1210-52/ME:5#
```

delete arpentry	
Purpose	To remove the entry for ARP table on the Switch.
Syntax	**delete arpentry [<ipaddr> | all]**
Description	The **delete arp_aging time** command is used to configure the entry for ARP table on the Switch.
Parameters	*[<ipaddr>* | *all]* – Specifiy the IP address or all of ARP entry to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To remove the ARP entry:

```
DES-1210-52/ME:5# delete arpentry 10.90.90.94
Command: delete arpentry 10.90.90.94


Success.

DES-1210-52/ME:5#
```

show arpentry	
Purpose	To displays all ARP entries on the Switch.
Syntax	**show arpentry {information | interface_name {system} | ip_address <ipaddr> | mac_address <macaddr> | summary}**
Description	The **show arpentry** command displays all ARP entries on the Switch.
Parameters	*information* – Displays the information of ARP entry. *interface_name {system}* – Displays the interface name of ARP entry. *ip_address <ipaddr>* – Displays the IP address of ARP entry. *mac_address<macaddr>* – Displays the MAC address of ARP entry. *summary* – Displays the summary of ARP entry.
Restrictions	None.

Example usage:

To display all ARP entries information on the Switch:

```
DES-1210-52/ME:5# show arpentry information
Command: show arpentry information



ARP Configurations:
-------------------
 Maximum number of ARP request retries is 3
 ARP cache timeout is 1800 seconds

DES-1210-52/ME:5#
```

show arpentry aging_time

Purpose	To displays the ARP entry aging time on the Switch.
Syntax	**show arpentry aging_time**
Description	The **show arpentry aging_time** command displays the ARP entry aging time on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the ARP entry aging time on the Switch:

```
DES-1210-52/ME:5# show arpentry aging_time
Command: show arpentry aging_time

ARP Aging Time = 30 (minutes)

DES-1210-52/ME:5#
```

44

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	Parameter
create iproute	default <ipaddr> {<value 1-254>}
delete iproute	{default}
show iproute	{<ipaddr> | static}

Each command is listed in detail, as follows:

create iproute	
Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	**create iproute default <ipaddr> {<value 1-254>}**
Description	The **create iproute** command is used to create a default static IP route entry to the Switch's IP routing table.
Parameters	*default* – Specifies to create a default IP route entry. *<ipaddr>* − The gateway IP address for the next hop router. *<value 1-254>* − Allows the entry of a routing protocol metric entry, representing the number of routers between the Switch and the IP address above. The default setting is 1.
Restrictions	Only Administrator, operator and power user-level users can issue this command.

Example usage:

To add the default static address 10.90.90.92 to the routing table:

```
DES-1210-52/ME:5# create iproute default 10.90.90.92
Command: create iproute default 10.90.90.92



Success.
DES-1210-52/ME:5#
```

delete iproute

Purpose	Used to delete an IP route entry from the Switch's IP routing table.
Syntax	**delete iproute {default}**
Description	The **delete iproute** command will delete an existing IP route entry from the Switch's IP routing table.
Parameters	{*default*} – Specifies to delete a default IP route entry.
Restrictions	Only Administrator, operator and power user-level users can issue this command.

Example usage:

To delete the default Gateway from the routing table:

```
DES-1210-52/ME:5# delete iproute
Command: delete iproute



Success.
DES-1210-52/ME:5#
```

show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	**show iproute {<ipaddr> | static}**
Description	The **show iproute** command will display the Switch's current IP routing table.
Parameters	<*ipaddr*> - Enter the IP address used here. *static* – Specifies to display all the static routes.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DES-1210-52/ME:5# show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway         Interface    Hops     Protocol
---------------------------   ---------------      -------------  ---------    ---------------


Total Entries  :0
DES-1210-52/ME:5#
```

45

STATIC MAC_BASED VLAN COMMANDS

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

Command	Parameter
create mac_based_vlan mac_address	<macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete mac_based_vlan	{mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]}
show mac_based_vlan mac_address	{mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]}

Each command is listed in detail, as follows:

create mac_based_vlan mac_address

Purpose	To create static MAC-based VLAN entries.
Syntax	**create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]**
Description	The **create mac_based_vlan mac_address** command is used to create static MAC-based VLAN entries.
Parameters	<*macaddr*> - Specify the MAC address to be created. <*vlan_name 32*> - Specify the VLAN name. The maximum length is 32 characters <*vlanid 1-4094*> - Specify the VLAN ID between 1 and 4094.
Restrictions	Only Administrator and operator-level users can issue this command.

Example usage:

To create a static MAC-based VLAN entry:

```
DES-1210-52/ME:5# create mac_based_vlan mac_address 00-00-00-00-00-01
vlan default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan
default



Success.

DES-1210-52/ME:5#
```

delete mac_based_vlan

Purpose	To delete static MAC-based VLAN entries.
Syntax	**delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]}**
Description	This **delete mac_based_vlan mac_address** command is used to delete static MAC-based VLAN entries.
Parameters	<*macaddr*> - Specify the MAC address to be deleted. <*vlan_name 32*> - Specify the VLAN name. The maximum length is 32 characters <*vlanid 1-4094*> - Specify the VLAN ID between 1 and 4094.
Restrictions	None.

Example usage:

To delete a static MAC-based VLAN entry:

```
DES-1210-52/ME:5# delete mac_based_vlan
Command: delete mac_based_vlan



Success.

DES-1210-52/ME:5#
```

show mac_based_vlan

Purpose	To display static MAC-based VLAN entries.
Syntax	**show mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]}**
Description	This **show mac_based_vlan mac_address** command is used to display static MAC-based VLAN entries.
Parameters	<*macaddr*> - Specify the MAC address to be displayed. <*vlan_name 32*> - Specify the VLAN name. The maximum length is 32 characters <*vlanid 1-4094*> - Specify the VLAN ID between 1 and 4094.
Restrictions	None.

Example usage:

To display a static MAC-based VLAN entry:

```
DES-1210-52/ME:5# show mac_based_vlan
Command: show mac_based_vlan

  MAC Address     MAC Address Mask   VLAN ID Status   Type
----------------- -----------------  ------- ------   ------
00-00-00-11-22-33 FF-FF-FF-FF-FF-FF  1       Active   Static

Total Entries : 1

DES-1210-52/ME:5#
```

46

D-LINK UNIDIRECTIONAL LINK DETECTION (DULD) COMMANDS

The D-Link Unidirectional Link Detection (DULD) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config duld ports	[<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}
show duld ports	{<portlist> | all}
config duld recover_timer	[0 | <sec 60-1000000>]
show duld recover_timer	

Each command is listed in detail, as follows:

config duld ports	
Purpose	To configure unidirectional link detection on ports.
Syntax	**config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}**
Description	Unidirectional link detection provides discovery mechanism based on 802.3ah to discovery its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.
Parameters	*[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be configured. *state [enable* | *disable]* – Specifies the unidirectional link detection status to be enabled or disabled. *mode [shutdown* | *normal]* – Specifies the mode the unidirectional link detection will be set to. ● *shutdown* – If any unidirectional link is detected, disable the port and log an event. ● *normal* – Only log an event when a unidirectional link is detected. *discovery_time <sec 5-65535>* – Enter the discovery time value here. This value must be between 5 and 65535.
Restrictions	Only Administrator and operator-level users can issue this command.

Example usage:

To enable unidirectional link detection on port 1:

```
DES-1210-52/ME:5# config duld ports 1 state enable
Command: config duld ports 1 state enable



Success.
DES-1210-52/ME:5#
```

show duld ports

Purpose	To show unidirectional link detection information.
Syntax	**show duld ports {<portlist> | all}**
Description	This **show duld ports** command is used to show unidirectional link detection information.
Parameters	*[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be displayed.
Restrictions	None.

Example usage:

To show unidirectional link detection information of port 1:

```
DES-1210-52/ME:5# show duld ports 1
Command: show duld ports 1

port   Admin State  Oper Status  Mode     Link Status    Discovery Time(Sec)
------ ------------------ ----------------- --------   -----------------   -------------------
1      Enabled      Disabled     Normal   Unknown        10
DES-1210-52/ME:5#
```

config duld recover_timer

Purpose	To configure unidirectional link detection recover time.
Syntax	**config duld recover_timer [0 | <sec 60-1000000>]**
Description	The **config duld recover_timer** command is used to configure unidirectional link detection recover time.
Parameters	*[0* | *<sec 60-1000000>]* – Specifies the recover time of unidirectional link detection function.
Restrictions	Only Administrator and operator-level users can issue this command.

Example usage:

To configure the unidirectional link detection recovery time to 100 seconds:

```
DGS-1210-28P/ME:5# config duld recover_timer 100
Command: config duld recover_timer 100


Success.

DGS-1210-28P/ME:5#
```

show duld recover_timer

Purpose	To display unidirectional link detection recover time.
Syntax	**show duld recover_timer**
Description	The **show duld recover_timer** command is used to display unidirectional link detection recover time.
Parameters	*[0* | *<sec 60-1000000>]* – Specifies the recover time of unidirectional link detection function.
Restrictions	None.

Example usage:

To display the unidirectional link detection recovery time:

```
DGS-1210-28P/ME:5# show duld recover_timer
Command: show duld recover_timer


DULD Recover Time   : 100


DGS-1210-28P/ME:5#
```

47

IPV6 NEIGHBOR DISCOVERY COMMANDS

The IPv6 Neighbor Discovery commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create ipv6 neighbor_cache	ipif System <ipv6_addr> <mac_addr>
delete ipv6 neighbor_cache	[ipif system | all] [<ipv6_addr> | static | dynamic | all]
show ipv6 neighbor_cache	[<ipif_name 12> | all] [ipv6address <ipv6_addr> | static | dynamic | all]
show ipv6 nd	
config ipv6 nd ns ipif System	retrans_time <integer 1-3600>
create ipv6route default	<ipv6addr>
delete ipv6route default	
show ipv6route	
enable ipif_ipv6_link_local_auto System	
disable ipif_ipv6_link_local_auto System	

Each command is listed in detail, as follows:

create ipv6 neighbor_cache	
Purpose	Used to add a static neighbor on an IPv6 interface.
Syntax	**create ipv6 neighbor_cache ipif System <ipv6_addr> <mac_addr>**
Description	This **create ipv6 neighbor_cache** command is used to add a static neighbor on an IPv6 interface.
Parameters	*<ipv6_addr>* –The IPv6 address of the neighbor. *<mac_addr>* –The MAC address of the neighbor.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a static neighbor cache entry on the interface System, with an IPv6 address of 3ffc::1 and a MAC address of 00:01:02:03:04:05:

```
DES-1210-52/ME:5# create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05
Command: create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05



Success.

DES-1210-52/ME:5#
```

delete ipv6 neighbor_cache

Purpose	Used to remove a static neighbor on an IPv6 interface.
Syntax	**delete ipv6 neighbor_cache [ipif system | all] [<ipv6_addr> | static | dynamic]**
Description	This **delete ipv6 neighbor_cache** command is used to remove a static neighbor on an IPv6 interface.
Parameters	*<ipv6_addr>* –The IPv6 address of the neighbor. *static* – Delete matching static entries. *dynamic* – Delete matching dynamic entries. *all* – All entries including static and dynamic entries will be deleted.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a static neighbor cache entry on the interface System, with an IPv6 address of 3ffc::1:

```
DES-1210-52/ME:5# delete ipv6 neighbor_cache 3ffc::1
Command: delete ipv6 neighbor_cache 3ffc::1



Success.

DES-1210-52/ME:5#
```

show ipv6 neighbor_cache

Purpose	Used to display the IPv6 neighbor cache.
Syntax	**show ipv6 neighbor_cache [<ipif_name 12> | all] [ipv6address <ipv6_addr> | static | dynamic | all]**
Description	This **show ipv6 neighbor_cache** command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all static entries, all dynamic entries, or all entries.
Parameters	*<ipif_name 12>* –The IPv6 interface name. *all* - Displays all interfaces. *ipv6address <ipv6_addr>* –The IPv6 address of the neighbor. *static* – Display all static neighbor cache entries. *dynamic* – Display all dynamic entries. *all* – Displays all entries including static and dynamic entries.
Restrictions	None.

Example usage:

To show all neighbor cache entries on the switch:

```
DES-1210-52/ME:5# show ipv6 neighbor_cache ipif all all
Command: show ipv6 neighbor_cache ipif all all



   IPv6 Address              Link-layer Addr    State    Interface
   ------------               ---------------------    --------   ---------------


Total Entries: 0
DES-1210-52/ME:5#
```

show ipv6 nd

Purpose	Used to display information regarding neighbor detection on the switch.
Syntax	**show ipv6 nd**
Description	This **show ipv6 nd** command is used to display information regarding neighbor detection on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show IPv6 ND related configuration:

```
DES-1210-52/ME:5# show ipv6 nd
Command: show ipv6 nd

Interface Name                : System
NS Retransmit Time            : 1(ms)

DES-1210-52/ME:5#
```

config ipv6 nd ns ipif System

Purpose	Configures the IPv6 ND neighbor solicitation retransmit time，which is the time between the retransmission of neighbor solicitation messages to a neighbor, when resolving the address or when probing the reachability of a neighbor.
Syntax	**config ipv6 nd ns ipif System retrans_time <integer 1-3600>**
Description	This **show ipv6 neighbor_cache** command is used to configures the retransmit time of IPv6 ND neighbor solicitation
Parameters	*retrans_time <integer 1 - 3600>* – Neighbor solicitation's retransmit timer in milliseconds. It has the same value as the RA retrans_time in the config IPv6 ND RA command. If the retrans_time parameter is configured in one of the commands, the retrans_time value in the other command will also change so that the values in both commands are the same. The range if 1 to 3600.

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

Example usage:

To configure the retrans_time of IPv6 ND neighbor solicitation to be 100:

```
DES-1210-52/ME:5# config ipv6 nd ns ipif System retrans_time 100
Command: config ipv6 nd ns ipif System retrans_time 100



Success.
DES-1210-52/ME:5#
```

create ipv6route default

Purpose	Used to create IPv6 route entries to the Switch’s IP routing table.
Syntax	**create ipv6route default <ipv6addr>**
Description	This **create ipv6route default** command is used to create a primary and backup IP route entry to the Switch’s IP routing table.
Parameters	*<ipv6addr>* – Specify the IPv6 address to be creted.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add a single static IPv6 entry in IPv6 format:

```
DES-1210-52/ME:5# create ipv6route default 3ffc::1
Command: create ipv6route default 3ffc::1



Success.
DES-1210-52/ME:5#
```

delete ipv6route default

Purpose	Used to delete a static IPv6 route entry from the Switch’s IP routing table.
Syntax	**delete ipv6route default**
Description	This **delete ipv6route default** command will delete an existing static IPv6 entry from the Switch’s IP routing table.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To o delete a static IPv6 entry from the routing table:

```
DES-1210-52/ME:5# delete ipv6route default
Command: delete ipv6route default



Success.
DES-1210-52/ME:5#
```

show ipv6route

Purpose	Used to display a static IPv6 route entry from the Switch’s IP routing table.
Syntax	**show ipv6route**
Description	This **delete ipv6route** command will display an existing static IPv6 entry from the Switch’s IP routing table.
Parameters	None.
Restrictions	None.

Example usage:

To o show a static IPv6 entry from the routing table:

```
DES-1210-52/ME:5# show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                    Protocol: Static Metric: 1
Next Hop   : 3ffc::1                   IPIF    : System

Total Entries: 1 DES-1210-52/ME:5#
```

enable ipif_ipv6_link_local_auto System

Purpose	Used to enable the autoconfiguration of the link local address when no IPv6 address is configured.
Syntax	**enable ipif_ipv6_link_local_auto System**
Description	This **enable ipif_ipv6_link_local_auto System** command will automatically create an IPv6 link local address for the Switch if no IPv6 address has previously been configured.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the IP interface IPv6 link-local settings on the switch:

```
DES-1210-52/ME:5# enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System



Success.
DES-1210-52/ME:5#
```

disable ipif_ipv6_link_local_auto System

Purpose	Used to disable the autoconfiguration of the IPv6 link local address.
Syntax	**disable ipif_ipv6_link_local_auto System**
Description	This **disable ipif_ipv6_link_local_auto System** command will disable the automatic creation of an IPv6 link local address for the Switch. Once this command is entered, any previous IPv6 link local address that has been created for the IP interface selected will be deleted from the switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the IP interface IPv6 link-local settings on the switch:

```
DES-1210-52/ME:5# disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System


Success.
DES-1210-52/ME:5#
```

48

BANNER COMMANDS

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

Command	Parameter
config log_save_timing	[log_trigger | on_demand | time_interval <minutes 1-65535>]
show log_save_timing	
show log_software_module	
show log	{index <value 1-500> - <value 1-500> | module <string 32> | severity [warning | all | informational]}

Each command is listed in detail, as follows:

config log_save_timing	
Purpose	Used to configure the method of saving logs to the Switch's Flash memory.
Syntax	**config log_save_timing [log_trigger | on_demand | time_interval <minutes 1-65535>]**
Description	This **config log_save_timing** command is used to configure the method used in saving logs to the Switch's Flash memory.
Parameters	*log_trigger* – Users who choose this method will have logs saved to the Switch every time a log event occurs on the Switch. *on_demand* – Users who choose this method will only save logs when they manually tell the Switch to do so, using the save all or save log command. *time_interval <minutes 1-65535>* – Use this parameter to configure the time interval that will be implemented for saving logs. The logs will be saved every x number of minutes that are configured here.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the time interval as every 30 minutes for saving logs:

```
DES-1210-52/ME:5# config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

DES-1210-52/ME:5#
```

show log_save_timing

Purpose	Used to show the log save timing.
Syntax	**show log_save_timing**
Description	This command allows display of the log save timing on the Switch.
Parameters	None.
Restrictions	None.

Usage Example:

To show the login save timing:

```
DES-1210-52/ME:5# show log_save_timing
Command: show log_save_timing

Saving log method: on_demand
DES-1210-52/ME:5#
```

show log_software_module

Purpose	Used to show the log software module.
Syntax	**show log_software_module**
Description	This command allows display of the log software module on the Switch.
Parameters	None.
Restrictions	None.

Usage Example:

To show the log software module:

```
DES-1210-52/ME:5# show log_software_module
Command: show log_software_module

CLI    SYSTEM

DES-1210-52/ME:5#
```

show log	
Purpose	Used to show the log.
Syntax	**show log {index <value 1-500> - <value 1-500> | module <string 32> | severity [warning | all | informational]}**
Description	This command allows display the log.
Parameters	*index <value 1-500>* – Specifies the index of logs to be displayed. *module <string 32>* – Specifies the module of logs to be displayed. *severity [warning* | *all* | *informational]* – Specifies the severity of logs to be displayed.
Restrictions	None.

Usage Example:

To show the log on the Switch:

```
DES-1210-52/ME:5# show log
Command: show log

Index  Time                Log Text
-----  ------------------- ----------------------------------------
  2    Jan  1 00:00:24     :CLI-6:Success.ful login through console port( User:
Anonymous )
  1    Jan  1 00:00:10     :SYSTEM-2:System started up
DES-1210-52/ME:5#
```

49

COMMAND HISTORY LIST COMMANDS

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

Command	Parameter
?	
show command_history	
dir	

Each command is listed in detail, as follows:

?	
Purpose	To display all commands in the Command Line Interface (CLI).
Syntax	**?**
Description	The **?** command displays all of the commands available through the Command Line Interface (CLI).
Parameters	*{<command>}* – Lists all the corresponding parameters for the specified command, along with a brief description of the command's 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-1210-52/ME:5# ?

Command: ?


?
CPU_Loading
cable diagnostic port
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear ethernet_oam ports
clear fdb
clear flood_fdb
clear igmp_snooping data_driven_group
clear log
clear mld_snooping data_driven_group
clear tech support
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode ports
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x fwd_pdu system
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

show command_history

Purpose	To display the command history.
Syntax	**show command_history**
Description	The **show command_history** command displays the command history.
Parameters	None.
Restrictions	None.

Example usage:

To display the command history:

```
DES-1210-52/ME:5# show command_history
Command: show command_history


?
config 802.1pq
show log_software_module
config log_save_timing log_trigger
config ipv6 nd ns ipif System retrans_time qinteger 1-3600>
```

```
create ipv6 neighbor_cache ipif System 3000::2 00-00-00-11-22-
33
show duld ports
config duld ports all discovery_time shoc 5-65535>



DES-1210-52/ME:5#
```

dir

Purpose	To display all commands.
Syntax	**dir**
Description	The **dir** command displays all commands.
Parameters	None.
Restrictions	None.

Example usage:

To display all of the commands:

```
DES-1210-52/ME:5# dir
Available commands:
?             CPU_Loading      cable          clear
config          create         delete         disable
download          enable          logout          ping
ping6           reboot         reload         reset
save            show           smtp           telnet
test           upload
DES-1210-52/ME:5#
```

50

SSH COMMANDS

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

Command	Parameter
enable ssh	
disable ssh	
config ssh algorithm	[3DES | MD5 | RSA | SHA1] [disable | enable]
config ssh authmode	[publickey | hostbased | password] [enable | disable]
show ssh authmode	
config ssh server	[authfail <int 2-20> | contimeout <sec 120-600> | maxsession <int 1-4> | rekey [10min | 30min | 60min | never]]
show ssh server	
show ssh algorithm	
config ssh user	<string 15> authmode [hostbased hostname <domain_name 32> hostname_IP <ip_addr> | password | publickey]
show ssh user authmode	

Each command is listed in detail, as follows:

enable ssh	
Purpose	To enable SSH.
Syntax	**enable ssh**
Description	The **enable ssh** command enables SSH on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable SSH:

```
DES-1210-52/ME:5# enable ssh
Command: enable ssh

Success.

The SSH server is enabled.

DES-1210-52/ME:5#
```

disable ssh

Purpose	To disable SSH.
Syntax	**disable ssh**
Description	The **disable ssh** command disables SSH on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable SSH:

```
DES-1210-52/ME:5# disable ssh
Command: disable ssh

Success.

The SSH server is disable.

DES-1210-52/ME:5#
```

config ssh algorithm

Purpose	To configure the SSH algorithm.
Syntax	**config ssh algorithm [3DES | MD5 | RSA | SHA1] [disable | enable]**
Description	The **config ssh algorithm** command configures the SSH algorithm setting on the Switch.
Parameters	Select the algorithm to be disabled or enabled: ▪ *3DES* – Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. ▪ *MD5* – Hash for Message Authentication Code (HMAC) MD5 Message Digest (MD5) mechanism. ▪ *RSA* – Hash for Message Authentication Code (HMAC) mechanism utilizing the RSA encryption algorithm. ▪ *SHA1* – Hash for Message Authentication Code (HMAC) Secure Hash Algorithm (SHA) mechanism. *[disable* | *eanble]* – Enables or Disables the SSH algorithm on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure SSH algorithm:

```
DES-1210-52/ME:5# config ssh algorithm 3DES enable
Command: config ssh algorithm 3DES enable

Success.

DES-1210-52/ME:5#
```

config ssh authmode

Purpose	To configure the SSH authentication mode setting.
Syntax	**config ssh authmode [publickey | hostbased | password] [enable | disable]**
Description	The **config ssh authmode** command configures the SSH authentication mode for users attempting to access the Switch.
Parameters	*publickey [enable* | *disable]* – Specifies that a publickey configuration set on a SSH server is to be used for authentication. Enables or disables SSH authentication on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the SSH authentication mode:

```
DES-1210-52/ME:5# config ssh authmode password enable
Command: config ssh authmode password enable



 Success.
DES-1210-52/ME:5#
```

show ssh authmode

Purpose	To display the SSH authentication mode setting.
Syntax	**show ssh authmode**
Description	The **show ssh authmode** command displays the current SSH authentication set on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the cuurent authentication mode set on the Switch:

```
DES-1210-52/ME:5# show ssh authmode
Command: show ssh authmode

The SSH Authmode :
------------------------------------------------------------
Password   : Enabled
Publickey  : Enabled
Hostbased  : Disabled
Success.
DES-1210-52/ME:5#
```

config ssh server

Purpose	To configure the SSH server.
Syntax	**config ssh server [authfail <int 2-20> | contimeout <sec 120-600> | maxsession <int 1-4> | rekey [10min | 30min | 60min | never]]**
Description	The **config ssh server** command configures the SSH server.
Parameters	*authfail <int 2-20>* - Specifies the authfail times. The value may be between 2 and 20 times. *contimeout <sec 120-600>* - Specifies the connection timeout. The value may be between 120 and 600 seconds. The default is 600 seconds. *maxsession <int 1-4>* – Specifies the maxseeion of ssh server. rekey [10min | 30min | 60min | never] – Specifies the rekey time. The possible values are 10min, 30min, 60min and never.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the SSH server:

```
DES-1210-52/ME:5# config ssh server authfail 20 maxsession 1
Command: config ssh server authfail 20 maxsession 1



 Success.
DES-1210-52/ME:5#
```

show ssh server

Purpose	To display the SSH server setting
Syntax	**show ssh server**
Description	The **show ssh server** command displays the current SSH server settings.
Parameters	None.
Restrictions	None.

Example usage:

To display the SSH server:

```
DES-1210-52/ME:5# show ssh server
Command: show ssh server

The SSH Server Configuration :
Max Session                    : 1
Connection Timeout             : 120
Authfail Attempts              : 20
Rekey Timeout                  : never
Success.

DES-1210-52/ME:5#
```

show ssh algorithm

Purpose	To display the SSH algorithm setting.
Syntax	**show ssh algorithm**
Description	The **show ssh algorithm** command displays the current SSH algorithm setting status.
Parameters	None.
Restrictions	None.

Example usage:

To display SSH algorithms cuurently set on the Switch:

```
DES-1210-52/ME:5# show ssh algorithm
Command: show ssh algorithm


Encryption Algorithm
-----------------------------
DES      : Enabled
3DES     : Enabled

Data Integrity Algorithm
-----------------------------
MD5      : Enabled
SHA1     : Enabled

Public Key Algorithm
-----------------------------
RSA      : Disabled
Success.

DES-1210-52/ME:5#
```

config ssh user

Purpose	To specify which SSH public key is manually configured.
Syntax	**config ssh user <string 15> authmode [hostbased hostname <domain_name 32> hostname_IP <ip_addr> | password | publickey]**
Description	The **config ssh crypto** command specifies which SSH public key is manually configured.
Parameters	*<string 15>* – Specifies the name of SSH user. *hostabsed hostname <domain_name 32>* – The username of the remote SSH client. *hostname_IP <ip_addr>* – The IP adderss of the remote SSH client. *[hostabsed* | *password* | *publickey]* – Specifies which configuration will be set on a SSH server for authentication.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the SSH user:

```
DES-1210-52/ME:5# config ssh user dlink authmode publickey
Command: config ssh user dlink authmode publickey

Success.

DES-1210-52/ME:5#
```

show ssh user authmode

Purpose	To display the SSH public key stored on the device.
Syntax	**show ssh user authmode**
Description	The **show ssh user authmode** command displays the SSH user stored on the device.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the SSH public key on the device:

```
DES-1210-52/ME:5# show ssh user authmode
Command: show ssh user authmode

Account is empty!
Total Entries: 0

Success.

DES-1210-52/ME:5#
```

51

SSL COMMANDS

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

Command	Parameter
enable ssl	{ciphersuite [DH-RSA-3DES-SHA1 | DH-RSA-DES-SHA1 | RSA-3DES-SHA1 | RSA-DES-SHA1 | RSA-EXP1024-DES-SHA1 | RSA-NULL-MD5 | RSA-NULL-SHA1]}
disable ssl	{ciphersuite [DH-RSA-3DES-SHA1 | DH-RSA-DES-SHA1 | RSA-3DES-SHA1 | RSA-DES-SHA1 | RSA-EXP1024-DES-SHA1 | RSA-NULL-MD5 | RSA-NULL-SHA1]}
show ssl	
download ssl certificate	[<ipaddr> | <ip6_addr>] certfilename <path_filename 64>

Each command is listed in detail, as follows:

enable ssl	
Purpose	To enable the SSL function on the Switch.
Syntax	**enable ssl {ciphersuite [DH-RSA-3DES-SHA1 | DH-RSA-DES-SHA1 | RSA-3DES-SHA1 | RSA-DES-SHA1 | RSA-EXP1024-DES-SHA1 | RSA-NULL-MD5 | RSA-NULL-SHA1]}**
Description	The **enable ssl** command enables SSL on the Switch by implementing every combination of listed ciphersuites on the Switch. Entering this command enables the SSL status on the Switch. Enabling SSL disables 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: ● DH-RSA-3DES-SHA1 ● DH-RSA-DES-SHA1 ● RSA-3DES-SHA1 ● RSA-DES-SHA1 ● RSA-EXP1024-DES-SHA1 ● RSA-NULL-MD5 ● RSA-NULL-SHA1 The ciphersuites are enabled by default on the Switch, yet the SSL status is disabled by default. Enabling SSL with a ciphersuite will not enable the SSL status on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DES-1210-52/ME:5# enable ssl
Command: enable ssl

Note: HTTP will be disabled if SSL is enabled.
Success.
DES-1210-52/ME:5#
```

disable ssl

Purpose	To disable the SSL function on the Switch.
Syntax	**disable ssl {ciphersuite [DH-RSA-3DES-SHA1 | DH-RSA-DES-SHA1 | RSA-3DES-SHA1 | RSA-DES-SHA1 | RSA-EXP1024-DES-SHA1 | RSA-NULL-MD5 | RSA-NULL-SHA1]}**
Description	The **disable ssl** command disables SSL on the Switch and can be used to disable all combinations of listed ciphersuites on the Switch. Note that disabling SSL will not enable WEB access automatically (WEB access will stay disabled), and you'll need to enable it manually.
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: ● DH-RSA-3DES-SHA1 ● DH-RSA-DES-SHA1 ● RSA-3DES-SHA1 ● RSA-DES-SHA1 ● RSA-EXP1024-DES-SHA1 ● RSA-NULL-MD5 ● RSA-NULL-SHA1
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DES-1210-52/ME:5# disable ssl
Command: disable ssl

Success.
DES-1210-52/ME:5#
```

show ssl

Purpose	To view the SSL status and the certificate file status on the Switch
Syntax	**show ssl**
Description	The **show ssl** command displays the SSL status and the certificate file status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DES-1210-52/ME:5# show ssl
Command: show ssl


SSL Status                         Enabled
RSA-NULL-MD5             0x0001  Enabled
RSA-NULL-SHA1            0x0002  Enabled
RSA-DES-SHA1             0x0004  Enabled
RSA-3DES-SHA1            0x0008  Enabled
DH-RSA-DES-SHA1          0x0010  Enabled
DH-RSA-3DES-SHA1         0x0020  Enabled
RSA-EXP1024-DES-SHA1     0x0040  Enabled

Success.
DES-1210-52/ME:5#
```

download ssl certificate

Purpose	To download ssl certificate file on the Switch.
Syntax	**download ssl certificate [<ipaddr> | <ip6_addr>] certfilename <path_filename 64>**
Description	The **download ssl certificate** command downloads the SSL file on the Switch.
Parameters	*<ipaddr>* – Specifies the IPv4 address of SSL file. *<ip6_addr>* – Specifies the IPv6 address of SSL file. *<path_filename 64>* –The DOS path and filename of the SSL file, up to 64 characters, on the TFTP server. For example, C:\1210.had.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To download SSL on the Switch:

```
DES-1210-52/ME:5# download ssl certificate 10.48.47.22 certfilename
1210.had
Command: download ssl certificate 10.48.47.22 certfilename 1210.had

Success.
DES-1210-52/ME:5#
```

52

ACCESS AUTHENTICATION CONTROL COMMANDS

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

Command	Parameter
create authen_login method_list_name	<string 15>
config authen_login	[default | method_list_name <string 15>] method [tacacs+ | radius | local | server_group <string 15> | none]
delete authen_login method_list_name	<string 15>
show authen_login	[all | default | method_list_name <string 15>]
show authen_policy	
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs+ | radius | local | server_group <string 15> | none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[all | default | method_list_name <string 15>]
enable authen_policy	
disable authen_policy	
config authen application	{console | http | ssh | telnet | all] [login | enable] [default | method_list_name <string 15>]
show authen application	
config authen parameter	[attempt <int 1-255> | response_timeout <int 0-255>]
show authen parameter	
create authen server_host	[<ipaddr> | ipv6address <ipv6addr>] protocol [radius | tacacs+] {port <int 1-65535> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	[<ipaddr> | ipv6address <ipv6addr>] protocol [tacacs+ | radius] {port <int 1-65535> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
delete authen server_host	[<ipaddr> | ipv6address <ipv6addr>] protocol [tacacs+ | radius]
show authen server_host	
create authen server_group	<string 15>

Command	Parameter
config authen server_group	[<string 15> | radius | tacacs+] [add | delete] server_host [<ipaddr> | ipv6address <ipv6addr>] protocol [radius | tacacs+]
delete authen server_group	<string 15>
show authen server_group	{<string 15>}
enable admin	
config admin local_enable	

Each command is listed in detail, as follows:

create authen_login method_list_name

Purpose	To create a user-defined list of authentication methods for users logging on to the Switch.
Syntax	**create authen_login method_list_name <string 15>**
Description	The **create authen_login method_list_name** command creates a list of 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>* - Defines the *method_list_name* to be created as a string of up to 15 alphanumeric characters.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the method list 'Trinity':

```
DES-1210-52/ME:5# create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity



Success.

DES-1210-52/ME:5#
```

config authen_login

Purpose	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+ | radius | local | server_group <string 15> | none]**
Description	The **config authen_login** command configures a user-defined or default *method list* of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command

	affects the authentication result. For example, if a user enters a sequence of methods like *tacacs – local,* the Switch sends an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the Switch sends an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. When the local method is used, the privilege level is dependant on the local account privilege configured on the Switch. Success.ful login using any of these methods gives the user a 'user' priviledge 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 more of the following authentication methods: ▪ *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. ▪ *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. ▪ *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. ▪ *server_group <string 15>* –Specifies that the user is to be authenticated using the server group *account* database on the Switch. ▪ *none* – Specifies that no authentication is required to access the Switch. *method_list_name <string 15>* – Specifies a previously created method list name defined by the user. One or more of the following authentication methods may be added to this method list: ▪ *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from a remote TACACS+ server. ▪ *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from a remote RADIUS server. ▪ *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. ▪ *server_group <string 15>* –Specifies that the user is to be authenticated using the server group *account* database on the Switch. ▪ *none* – Specifies that no authentication is required to access the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user defined method list 'Trinity' with authentication methods TACACS+, RADIUS and local, in that order.

```
DES-1210-52/ME:5# config authen_login method_list_name Trinity method tacacs+
radius local
Command: config authen_login method_list_name Trinity method tacacs+ radius local



Success.

DES-1210-52/ME:5#
```

delete authen_login method_list_name

Purpose	To delete a previously configured user defined list of authentication methods for users logging on to the Switch.
Syntax	**delete authen_login method_list_name <string 15>**
Description	The **delete authen_login method_list_name** command deletes a list of authentication methods for user login.
Parameters	*<string 15>* - The previously created *method_list_name* to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the method list name 'Trinity':

```
DES-1210-52/ME:5# delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DES-1210-52/ME:5#
```

show authen_login

Purpose	To display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**show authen_login [all | default | method_list_name <string 15>]**
Description	The **show authen_login** command displays a list of authentication methods for user login.
Parameters	*default* – Displays the default method list for users logging on to the Switch. *method_list_name <string 15>* - Specifies the *method_list_name* to display. *all* – Displays all the authentication login methods currently configured on the Switch. The command displays the following parameters: • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemeted, per method list name.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view all authentication login method list names:

```
DES-1210-52/ME:5# show authen_login all
Command: show authen_login all


Method List Name  Priority   Method Name   Comment
-------------------------  ----------   ---------------      ------------------
default            1          local           Keyword
Trinity            1          tacacs+         Built-in Group
                   2          radius          Built-in Group
                   3          local           Keyword

DES-1210-52/ME:5#
```

show authen_policy

Purpose	Used to display the system access authentication policy status on the Switch.
Syntax	**show authen_policy**
Description	The **show authen_policy** command display the system access authentication policy status on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the system access authentication policy:

```
DES-1210-52/ME:5# show authen_policy
Command: show authen_policy

Authentication Policy : Disabled

DES-1210-52/ME:5#
```

create authen_enable method_list_name

Purpose	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	The **create authen_enable method_list_name** command creates a list of authentication methods for promoting 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>* - Defines the *authen_enable method_list_name* to be created as a string of up to 15 alphanumeric characters.
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 Adminstrator privileges:

```
DES-1210-52/ME:5# create authen_enable method_list_name Permit
Command: create authen_enable method_list_name Permit

Success.

DES-1210-52/ME:5#
```

config authen_enable	
Purpose	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+ | radius | local | server_group <string 15> | none}**
Description	The **config authen_enable** command configures a user-defined list of authentication methods for promoting normal user 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 affects the authentication result. For example, if a user enters a sequence of methods like *tacacs+ – radius – local_enable,* the Switch sends an authentication request to the first *TACACS+* host in the server group. If no verification is found, the Switch sends 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 restarts the same sequence with the following protocol listed, *radius*. If no authentication takes place using the *radius* list, the *local_enable* password set in the Switch is used to authenticate the user. Success.ful authentication using any of these methods gives the user an ‘Admin’ level privilege.
Parameters	*default* – The default method list for adminstration rights authentication, as defined by the user. The user may choose one or more of the following authentication methods: • *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. • *radius* – Specifies that the user is to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. • *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch.

	• *server_group <string 15>* – Specifies the server group name for authentication. • *none* – Specifies that no authentication is required to access the Switch. *method_list_name <string 15>* – Specifies a previously created *authen_enable method_list_name*. The user may add one or more of the following authentication methods to this method list: • *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from a remote TACACS+ server. • *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from a remote RADIUS server. • *local* - Specifies that the user is 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. • *server_group <string 15>* –Specifies that the user is to be authenticated using the server group account database on the Switch. • *none* – Specifies that no authentication is required to access 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+, RADIUS and local_enable, in that order.

```
DES-1210-52/ME:5# config authen_enable method_list_name Trinity method
tacacs+ radius local
Command: config authen_enable method_list_name Trinity method tacacs+ radius
local

Success.

DES-1210-52/ME:5#
```

delete authen_enable method_list_name

Purpose	To delete a user-defined 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	The **delete authen_enable method_list_name** command deletes a user-defined list of authentication methods for promoting user level privileges to Adminstrator level privileges.
Parameters	*<string 15>* - The previously created *authen_enable method_list_name* to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user-defined method list 'Permit'

```
DES-1210-52/ME:5# delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit


Success.

DES-1210-52/ME:5#
```

show authen_enable

Purpose	To display the list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**show authen_enable [all | default | method_list_name <string 15>]**
Description	The **show authen_enable** command deletes a user-defined list of authentication methods for promoting user level privileges to Adminstrator level privileges.
Parameters	*default* – Displays the default method list for users attempting to gain access to Administrator level privileges on the Switch. *method_list_name <string 15>* – The *method_list_name* to be displayed. *all* – Displays all the authentication login methods currently configured on the Switch. The command displays the following parameters: • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemeted, per method list name.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1210-52/ME:5# show authen_enable all
Command: show authen_enable all


Method List Name  Priority  Method Name   Comment
----------------   --------  -------------   -------------
default            1        local          Keyword

DES-1210-52/ME:5#
```

enable authen_policy

Purpose	To enable the authentication policy on the Switch.
Syntax	**enable authen_policy**
Description	The **enable authen_policy** command enables the authentication policy on the Switch.

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

Example usage:

To enable the authentication policy:

```
DES-1210-52/ME:5# enable authen_policy
Command: enable authen_policy

Success.
DES-1210-52/ME:5#
```

disable authen_policy

Purpose	To disable the authentication policy on the Switch.
Syntax	**disable authen_policy**
Description	The **disable authen_policy** command disables the authentication policy on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the authentication policy:

```
DES-1210-52/ME:5# disable authen_policy
Command: disable authen_policy

Success.
DES-1210-52/ME:5#
```

config authen application

Purpose	To configure various applications on the Switch for authentication using a previously configured method list.
Syntax	**config authen application {console | http | ssh | telnet | all] [login | enable] [default | method_list_name <string 15>]**
Description	The **config authen application** command configures Switch applications (console, Telnet, SSH) for login at the user level and at the administration level (*authen_enable*), utilizing a previously configured method list.
Parameters	*application* – Specifies the application to configure. One of the following four options may be selected: • *console* – Configures the command line interface login method. • *http* – Configures the http login method. • *ssh* – Configures the Secure Shell login method. • *telnet* – Configures the telnet login methods. • *all* – Configures all applications as (console, Telnet, SSH) login methods.

	login – Configures an application for normal login on the user level, using a previously configured method list. *enable* – Configures an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Configures an application for user authentication using the default method list. *method_list_name <string 15>* – Configures an application for user authentication using a previously configured *method_list_name*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the command line interface:

```
DES-1210-52/ME:5# config authen application http login default
Command: config authen application http login default



Success.
DES-1210-52/ME:5#
```

show authen application

Purpose	To display authentication methods for the various applications on the Switch.
Syntax	**show authen application**
Description	The **show authen application** command displays all of the authentication method lists (login, enable administrator privileges) for Switch configuration applications (console, Telnet, SSH) currently configured on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1210-52/ME:5# show authen application
Command: show authen application



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

DES-1210-52/ME:5#
```

config authen parameter

Purpose	To provide user to configure the authentication parameters on the Switch.
Syntax	**config authen parameter [attempt <int 1-255> | response_timeout <int 0-255>]**
Description	The **config authen parameter attempt** command provides user to configure the authentication parameters on the Switch.
Parameters	*attempt <integer 1-255>* – Specifies the attempt of authentication parameter on the Switch. The value range is between 1 and 255. *response_timout <integer 0-255>* – Specifies the response timout of authentication parameter on the Switch. The value range is between 0 and 255.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the command line interface:

```
DES-1210-52/ME:5# config authen parameter attempt 10
Command: config authen parameter attempt 10



Success.
DES-1210-52/ME:5#
```

show authen parameter

Purpose	To display authentication parameters for the various applications on the Switch.
Syntax	**show authen parameter**
Description	The **show authen parameter** command displays the authentication parameter on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the authentication parameters for all applications on the Switch:

```
DES-1210-52/ME:5# show authen parameter
Command: show authen parameter

Response Timeout : 30 seconds
User Attempts    : 3
DES-1210-52/ME:5#
```

create authen server_host

Purpose	To create an authentication server host.
Syntax	**create authen server_host [<ipaddr> | ipv6address <ipv6addr>]**

	protocol [radius | tacacs+] {port <int 1-65535> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
Description	The **create authen server_host** command creates an authentication server host for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server host on a remote host. The TACACS+/RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*[<ipaddr>* | *ipv6address <ipv6addr>]* – The IPv4 or IPv6 address of the remote server host to add. *protocol* – The protocol used by the server host. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol. *port <int 1-65535>* – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port number is 49 for TACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *key [<string 254>* | *none]* – The authentication key to be shared with a configured TACACS+ or RADIUS server only. The value is a string of up to 254 alphanumeric characters, or *none*. *timeout <int 1-255>* – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. This field is inoperable for the TACACS+ protocol.
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-1210-52/ME:5# 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

Key is empty for TACACS+ or RADIUS.
Retransmit is meaningless for TACACS+.

Success.

DES-1210-52/ME:5#
```

config authen server_host

Purpose	To configure a user-defined authentication server host.
Syntax	**config authen server_host [<ipaddr> | ipv6address <ipv6addr>] protocol [tacacs+ | radius] {port <int 1-65535> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}**
Description	The **config authen server_host** command configures a user-defined authentication server host for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server host on a remote host. The TACACS+/RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*[<ipaddr>* | *ipv6address <ipv6addr>]* – The IPv4 or IPv6 address of the remote server host the user wishes to alter. *protocol* – The protocol used by the server host. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • radius – Specifies that the server host utilizes the RADIUS protocol. *port <int 1-65535>* – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port number is 49 for TACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *key [<string 254>* | *none]* – The authentication key to be shared with a configured TACACS+ or RADIUS server only. The value is a string of up to 254 alphanumeric characters, or *none*. *timeout <int 1-255>* – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. 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-1210-52/ME:5# 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


Retransmit is meaningless for TACACS+.


Success.
DES-1210-52/ME:5#
```

delete authen server_host

Purpose	To delete a user-defined authentication server host.
Syntax	**delete authen server_host [<ipaddr> | ipv6address <ipv6addr>] protocol [tacacs+ | radius]**
Description	The **delete authen server_host** command deletes a user-defined authentication server host previously created on the Switch.
Parameters	*server_host [<ipaddr>* | *ipv6address <ipv6addr>]* - The IPv4 or IPv6 address of the remote server host to be deleted. *protocol* – The protocol used by the server host the user wishes to delete. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a user-defined RADIUS authentication server host:

```
DES-1210-52/ME:5# delete authen server_host 10.1.1.121 protocol radius
Command: delete authen server_host 10.1.1.121 protocol radius



Success.
DES-1210-52/ME:5#
```

show authen server_host

Purpose	To view a user-defined authentication server host.
Syntax	**show authen server_host**
Description	The **show authen server_host** command displays 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 include TACACS+ or RADIUS. Port – The virtual port number on the server host. The default value is 49.

	Timeout - The time in seconds the Switch waits for the server host to reply to an authentication request. Retransmit - The value in the retransmit field denotes how many times the device resends 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	Only Administrator-level users can issue this command.

Example usage:

To view authenticaion server hosts currently set on the Switch:

```
DES-1210-52/ME:5# show authen server_host
Command: show authen server_host


IP Address    Protocol   Port   Timeout  Retransmit  Key
---------------    --------------  ------   ------------ ----- ----------  --------------------


10.1.1.121      tacacs+    4321    ------      -1


Total Entries : 1

DES-1210-52/ME:5#
```

create authen server_group

Purpose	To create an authentication server host.
Syntax	**create authen server_group <string 15>**
Description	The **create authen server_ group** command creates an authentication server group for the protocols on the Switch.
Parameters	*<string 15>* – Defines the authentication group name as a string of up to 15 alphanumeric characters.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a server group “dlinkgroup”:

```
DES-1210-52/ME:5# create authen server_group dlinkgroup
Command: create authen server_group dlinkgroup



Success.
DES-1210-52/ME:5#
```

config authen server_group

Purpose	To configure a user-defined authentication server host.
Syntax	**config authen server_group [<string 15> | radius | tacacs+] [add | delete] server_host [<ipaddr> | ipv6address <ipv6addr>] protocol [radius | tacacs+]**
Description	The **config authen server_ group** command configures a user-defined authentication server group for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server group on a remote host. The TACACS+/RADIUS server group then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server group is 16.
Parameters	*<string 15>* – Defines the authentication group name as a string of up to 15 alphanumeric characters. *server_host [<ipaddr>* | *ipv6address <ipv6addr>]* – The IPv4 or IPv6 address of the remote server group the user wishes to alter. *[add* | *delete]* –Specifies the authentication server host will be add or deleted of the server group. *protocol* – The protocol used by the server host. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a RADIUS authentication server group:

```
DES-1210-52/ME:5# config authen server_group dlinkgroup add server_host
10.1.1.121 protocol radius
Command: config authen server_group dlinkgroup add server_host 10.1.1.121
protocol radius


Success.
DES-1210-52/ME:5#
```

delete authen server_group

Purpose	To delete a user-defined authentication server host.
Syntax	**delete authen server_group <string 15>**
Description	The **delete authen server_ group** command deletes a user-defined authentication server group previously created on the Switch.
Parameters	*<string 15>* –Specifies the authentication server group name to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a user-defined rd1 authentication server group:

```
DES-1210-52/ME:5# delete authen server_group dlinkgroup
Command: delete authen server_group dlinkgroup



Success.
DES-1210-52/ME:5#
```

show authen server_group

Purpose	To view a user-defined authentication server group.
Syntax	**show authen server_group {<string 15>}**
Description	The **show authen server_ group** command displays user-defined authentication server groups previously created on the Switch. The following parameters are displayed: Group Name – The name of the server group. IP Address – The IP address of the authentication server group. Protocol – The protocol used by the server group. Possible results include TACACS+ or RADIUS.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view authenticaion server hosts currently set on the Switch:

```
DES-1210-52/ME:5# show authen server_group
Command: show authen server_group

(1) Group Name: tacacs+

  IP Address: 10.0.0.2
    Protocol: tacacs+


(2) Group Name: radius

  (No servers in this group)


Total Entries : 2

DES-1210-52/ME:5#
```

enable admin

Purpose	To promote user level privileges to administrator level privileges.
Syntax	**enable admin**
Description	The **enable admin** command enables a user to be granted administrative privileges on to the Switch. After logging on to the Switch, users have only ‘user’ level privileges. To gain access to administrator level privileges, the user may enter this command. The system then prompts for an authentication password. Possible authentication methods for this function include TACACS, TACACS+, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because TACACS does not support the enable function, the user must create a special account on the server host which has the username ‘enable’, and a password configured by the administrator that will support the ‘enable’ function. This function becomes inoperable when the authentication policy is disabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable administrator privileges on the Switch:

```
DES-1210-52/ME:5# enable admin
Command: enable admin

Success.
DES-1210-52/ME:5#
```

config admin local_enable

Purpose	To configure the local_enable password for administrator level privileges.
Syntax	**config admin local_enable**
Description	The **config admin local_enable** command changes the locally enabled password for the **local_enable admin** command. When a user chooses the ‘*local_enable*’ method to promote user level privileges to administrator privileges, the user is prompted to enter the password configured here. After entering the **config admin local_enable** command, the user is prompted to enter the old password, then a new password in a string of no more than 15 alphanumeric characters, and finally prompted to enter the new password again for confirmation. See the example below.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the password for the ‘local_enable’ authentication method:

```
DES-1210-52/ME:5# 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-1210-52/ME:5#
```

53

LACP COMMANDS

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

Command	Parameter
config lacp port_priority	<portlist> <value 0-65535> [timeout <long | short>]
show lacp	{<portlist>}
config lacp_ports	<portlist> mode [active | passive]

Each command is listed in detail, as follows:

config lacp port_priority	
Purpose	To set the priority value of a physical port in an LACP group.
Syntax	**config lacp port_priority <portlist> <value 0-65535> [timeout <long | short>]**
Description	The **config lacp port_priority** command sets the LACP priority value and administrative timeout of a physical port or range of ports in an LACP group.
Parameters	<*portlist*> - A port or range of ports to be configured. <*value 0-65535*> - Specifies the LACP priority value for a port or range of ports to be configured. The default is 1. <*timeout*> - Specifies the administrative LACP timeout. • *long* – Specifies the LACP timeout to be 90 seconds. This is the default. • *short* – Specifies the LACP timeout to be 3 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the LACP priority of ports 1-5:

```
DES-1210-52/ME:5# config lacp port_priority 1-5 100 timeout long
Command: config lacp port_priority 1-5 100 timeout long



Success.
DES-1210-52/ME:5#
```

show lacp	
Purpose	To display current LACP port mode settings.
Syntax	**show lacp {<portlist>}**
Description	The **show lacp** command displays the current LACP mode settings.

Parameters	*<portlist>* - A port or range of ports whose LACP settings are to be displayed. If no parameter is specified, the system displays the current LACP status for all ports.
Restrictions	None.

Example usage:

To display LACP information for port1~3:

```
DES-1210-52/ME:5# show lacp 1-3
Command: show lacp 1-3

Port  Priority  Activity  Timeout
----- ---------- ----------- --------------
1      100        Active    Short (3 sec)
2      100        Active    Short (3 sec)
3      100        Active    Short (3 sec)
DES-1210-52/ME:5#
```

config lacp_ports

Purpose	To configure settings for LACP compliant ports.
Syntax	**config lacp_ports <portlist> mode [active | passive]**
Description	The **config lacp_ports** command is used to configure ports that have been previously designated as LACP ports.
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, operator or power user–level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DES-1210-52/ME:5# config lacp_ports 1 mode active
Command: config lacp_ports 1 mode active

Success.
DES-1210-52/ME:5#
```

54

LLDP COMMANDS

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

Command	Parameter
enable lldp	
disable lldp	
config lldp message_tx_interval	<sec 5-32768>
config lldp message_tx_hold_multiplier	<int 2-10>
config lldp reinit_delay	<sec 1-10>
config lldp tx_delay	<sec 1-8192>
config lldp notification_interval	<sec 5-3600>
show lldp	
show lldp ports	{<portlist>}
show lldp local_ports	{<portlist>} {mode[brief | normal | detailed]}
show lldp remote_ports	{<portlist>} {mode[brief | normal | detailed]}
config lldp ports	[<portlist> | all] notification [enable | disable]
config lldp ports	[<portlist> | all] admin_status [tx_only | rx_only | tx_and_rx | disable]
config lldp ports	[<portlist>|all] mgt_addr [ipv4 <ipaddr>| ipv6 <ipv6addr>] [enable | disable]
config lldp ports	[<portlist>|all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]
config lldp ports	[<portlist>|all] dot3_tlvs [all | link aggregation | mac_phy_configuration_status | maximum_frame_size | power_via_mdi] [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_pvid [disable | enable]
config lldp ports	[<portlist>|all] dot1_tlv_protocol_identity [all | eapol | gvrp | lacp | stp][disable | enable]
config lldp ports	[<portlist>|all] dot1_tlv_vlan_name [vlan <vlan_name 32> | vlanid <vidlist>] [disable | enable]
config lldp ports	[<portlist>|all] power_pse_tlv [enable | disable]
show lldp power_pse_tlv	
show lldp mgt_addr	{ipv4 <ipaddr> | ipv6 <ipv6addr>}
show lldp statistics	{ports <portlist>}

Each command is listed in detail, as follows:

enable lldp

Purpose	To enable LLDP on the switch.
Syntax	**enable lldp**
Description	The **enable lldp** command enables the *Link Layer Discovery Protocol* (LLDP) on the switch.
Parameters	None.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To enable LLDP on the switch:

```
DES-1210-52/ME:5# enable lldp
Command: enable lldp

Success.
DES-1210-52/ME:5#
```

disable lldp

Purpose	To disable LLDP on the switch.
Syntax	**disable lldp**
Description	The **disable lldp** command disables the *Link Discovery Protocol* (LLDP) on the switch.
Parameters	None.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To disable LLDP on the switch:

```
DES-1210-52/ME:5# disable lldp
Command: disable lldp

Success.
DES-1210-52/ME:5#
```

config lldp message_tx_interval

Purpose	To define the lldp message tx interval
Syntax	**config lldp message_tx_interval <sec 5-32768>**
Description	The **config lldp message_tx_interval** defines the lldp message interval of the incoming messages.
Parameters	*<sec 5-32768>* – Defines the message interval time. The range is between 5 and 32768.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure LLDP message tx interval on the switch:

```
DES-1210-52/ME:5# config lldp message_tx_interval 10
Command: config lldp message_tx_interval 10

Success.

DES-1210-52/ME:5#
```

config lldp message_tx_hold_multiplier

Purpose	To define the lldp hold-multiplier on the switch.
Syntax	**config lldp message_tx_hold_multiplier <int 2-10>**
Description	The **config lldp message_tx_hold_multiplier** command specifies the amount of time the receiving device should hold a *Link Layer Discovery Protocol* (LLDP) packet before discarding it.
Parameters	*message_tx_hold_multiplier (int 2-10)* – Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value. (Range: 2-10). The default configuration is 4.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP Message tx hold multiplier settings:

```
DES-1210-52/ME:5# config lldp message_tx_hold_multiplier 2
Command: config lldp message_tx_hold_multiplier 2


Success.

DES-1210-52/ME:5#
```

config lldp reinit_delay

Purpose	To define the lldp reinint–delay on the switch.
Syntax	**config lldp reinit_delay <sec 1-10>**
Description	The **lldp reinit_delay** *seconds* command specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.
Parameters	*<sec 1-10>* – Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 10 seconds. The default configuration is 2 seconds.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure LLDP reinit delay:

```
DES-1210-52/ME:5# config lldp reinit_delay 1
Command: config lldp reinit_delay 1


Success.

DES-1210-52/ME:5#
```

config lldp tx_delay

Purpose	To configure the lldp tx_delay on the switch.
Syntax	**config lldp tx_delay <sec 1-8192>**
Description	The **config lldp tx_delay** command specifies the delay between Success.ive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB, use the **lldp tx_delay** command in global configuration mode.
Parameters	*<sec 1-8192>* – Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 8192 seconds. The default configuration is 2 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP tx delay:

```
DES-1210-52/ME:5# config lldp tx_delay 1
Command: config lldp tx_delay 1


Success.

DES-1210-52/ME:5#
```

config lldp notification_interval

Purpose	To configure the timer of the notification interval used to send notifications to configured SNMP trap receiver(s).
Syntax	**config lldp notification_interval <sec 5-3600>**
Description	The **config lldp notification_interval** command globally changes the interval between Success.ive LLDP change notifications generated by the switch.
Parameters	*<sec 5-3600>* – The range is from 5 second to 3600 seconds. The default setting is 5 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To change the notification interval:

```
DES-1210-52/ME:5# config lldp notification_interval 10
Command: config lldp notification_interval 10


Success.

DES-1210-52/ME:5#
```

show lldp

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) on the switch.
Syntax	**show lldp**
Description	The **show lldp** displays the LLDP configuration on the switch.

Parameters	None.
Restrictions	None.

Example usage:

To show LLDP settings:

```
DES-1210-52/ME:5# show lldp
Command: show lldp

LLDP System Information
   Chassis Id Subtype       : MAC Address
   Chassis Id                : 00-01-02-03-04-05
   System Name              :
   System Description       : DES-1210-52/ME         7.00.004
   System Capabilities       : Bridge

LLDP Configurations
   LLDP Status               : Enable
   Message Tx Interval      : 10
   Message Tx Hold Multiplier: 2
   ReInit Delay              : 1
   Tx Delay                  : 1
   Notification Interval     : 5

DES-1210-52/ME:5#
```

show lldp ports

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) ports configuration on the switch.
Syntax	**show lldp ports {<portlist>}**
Description	The **show lldp ports** command displays the information regarding the ports.
Parameters	*<portlist>* − A port or range of ports to be displayed.
Restrictions	None.

Example usage:

To show the information for port 1:

```
DES-1210-52/ME:5# show lldp ports 1

Port ID              : 1
-----------------------------------------------------------------
Admin Status          : TX_and_RX
Notification Status     : Disable
Advertised TLVs Option  :
   Port Description                                   Disable
   System Name                                        Disable
   System Description                                  Disable
   System Capabilities                                Disable
   Enabled Management Address
      (NONE)
   Port VLAN ID                                       Disable
   Enabled Port_and_Protocol_VLAN_ID
      (None)
   Enabled VLAN Name
      (None)
   Enabled Protocol_Identity
      (None)
   MAC/PHY Configuration/Status                      Disable
   Power Via MDI                                     Disable
   Link Aggregation                                  Disable
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

show lldp local_ports

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) configuration that is advertised from a specific port.
Syntax	**show lldp local_ports {<portlist>} {mode[brief | normal | detailed]}**
Description	The **show lldp local_ports** command displays the configuration that is advertised from a specific port.
Parameters	*<portlist>* − A port or range of ports to be displayed. *{mode[brief* | *normal* | *detailed]}* − defines which mode of information want to be displayed, brief, normal or detailed.
Restrictions	None.

Example usage:

To show the local port information for port 1 with mode brief:

```
DES-1210-52/ME:5# show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief

Port ID : 1
--------------------------------------------
Port ID Subtype         : Local
Port ID               : Slot0/1
Port ID Desctiption       : D-Link DES-1210-52/ME Rev.C1/7.00.004 Port 1


DES-1210-52/ME:5#
```

show lldp remote_ports

Purpose	To display information regarding the neighboring devices discovered

	using LLDP.
Syntax	**show lldp remote_ports {<portlist>} {mode[brief | normal | detailed]}**
Description	The **show lldp remote_ports command** displays the information regarding neighboring devices.
Parameters	*<portlist>* − A port or range of ports to be displayed. *[mode[brief* | *normal* | *detailed]}* − defines which mode of information want to be displayed, brief, normal or detailed.
Restrictions	None.

Example usage:

To show the information for remote ports:

```
DES-1210-52/ME:5# show lldp remote_ports 1 mode normal
Command: show lldp remote_ports 1 mode normal

Port ID : 1
-----------------------------------------------------------------------
Remote Entities Count : 0
   (NONE)

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To enable LLDP notification on a port or ports.
Syntax	**config lldp ports [<portlist> | all] notification [enable | disable]**
Description	The **config lldp ports** notification command defines lldp notification per port on the switch.
Parameters	*ports [<portlist>* | *all]* – Specify a port or ports to be configured. *notification [enable* | *disable]*– defines is notification is enabled or disabled.
Restrictions	None.

Example usage:

To configure LLDP notification:

```
DES-1210-52/ME:5# config lldp ports 1-3 notification enable
Command: config lldp ports 1-3 notification enable


Success.

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To define LLDP admin status on a port or ports.
Syntax	**config lldp ports [<portlist> | all] admin_status [tx_only | rx_only | tx_and_rx | disable]**
Description	The **config lldp ports** admin status command defines lldp admin status per port on the switch.

Parameters	*[<portlist> | all]* – Specify a port or ports to be configured. *Admin status* – Defines admin status of ports on the switch. Tx- Tx only Rx – Rx only Both – Tx and RX Disable – admin status disabled.
Restrictions	None.

Example usage:

To configure LLDP admin status

```
DES-1210-52/ME:5# config lldp ports 2 admin_status disable
Command: config lldp ports 2 admin_status disable


Success.

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To define LLDP management address advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] mgt_addr [ipv4 <ipaddr>| ipv6 <ipv6addr>] [enable | disable]**
Description	The **config lldp ports** mgt_addr command defines if lldp will advertise the switch’s IP address the command is per port on the switch.
Parameters	*[<portlist> | all]* – Specify a port or ports to be configured. *mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>]* – defines wether the management address (IPv4 or IPv6 address) advertisement will be enabled or disabled
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP management address advertisement:

```
DES-1210-52/ME:5# config lldp ports 1 mgt_addr ipv4 100.1.1.2 enabled
Command: config lldp ports 1 mgt_addr ipv4 100.1.1.2 enabled


Success.

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]**
Description	The **config lldp ports** basic TLVs command defines if lldp will

	advertise the switch's basic TLVs the command is per port on the switch.
Parameters	*[<portlist>* | *all]* – Specify a port or ports to be configured. *Basic TLVs:* *all* – Advertisement of all the basic TLVs *port description* – Advertisement of *Port description* *system name* – Advertisement of *system name* *system description* – Advertisement of *System description* *system capabilities* – Advertisement of system capabilities
Restrictions	None.

Example usage:

To configure LLDP Basis TLVs

```
DES-1210-52/ME:5# config lldp ports 1 basic_tlvs all enable
Command: config lldp ports 1 basic_tlvs all enable


Success.

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] dot3_tlvs [all | link aggregation | mac_phy_configuration_status | maximum_frame_size | power_via_mdi] [enable | disable]**
Description	The **config lldp ports** dot3 TLVs command defines if lldp will advertise the mac_phy_configuration_status the command is per port on the switch.
Parameters	*[<portlist>* | *all]* – Specify a port or ports to be configured. *dot3_tlvs* – defines if the advertisement is enabled or disabled. The possible values are: link_aggregation, mac_phy_configuration_status, maximum_frame_size, power_via_mdi or all.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP mac_phy_configuration status:

```
DES-1210-52/ME:5# config lldp ports 2 dot3_tlvs mac_phy_configuration_status
enable
Command: config lldp ports 2 dot3_tlvsmac_phy_configuration_status enable


Success.

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_pvid [disable | enable]**
Description	The **config lldp ports** dot1 TLVs command defines if lldp will advertise the

	mac_phy_configuration_status the command is per port on the switch.
Parameters	*[<portlist>* | *all]* – Specify a port or ports to be configured. *[enable* | *disable]* - Defines if the advertisement is enabled or disabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP TLV PVID:

```
DES-1210-52/ME:5# config lldp ports all dot1_tlv_pvid disable
Command: config lldp ports all dot1_tlv_pvid disable


Success.

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_protocol_identity [all | eapol | gvrp | lacp | stp][disable | enable]**
Description	The **config lldp ports** dot1 TLVs command defines if lldp will advertise the mac_phy_configuration_status the command is per port on the switch.
Parameters	*[<portlist>* | *all]* – Specify a port or ports to be configured. *dot1_tlv_protocol_identity* − Defines if the advertisement is enabled or disabled. The possible values are: eapol, gvrp, lacp, stp or all.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP ports configuration status:

```
DES-1210-52/ME:5# config lldp ports all dot1_tlv_protocol_identity eapol enable
Command: config lldp ports all dot1_tlv_protocol_identity eapol enable


Success.

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_vlan_name [vlan <vlan_name 32> | vlanid <vidlist>] [disable | enable]**
Description	The **config lldp ports** dot1 TLVs command defines lldp admin status per port on the switch.
Parameters	*[<portlist>* | *all]* – Specify a port or ports to be configured. *vlan <vlan_name 32>* –The name of the VLAN to be configured. *dot1_tlv_vlan_name* − Defines if the advertisement is enabled or disabled. *vlanid <vidlist>* –The vid of the VLAN to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP mac_phy_configuration status:

```
DES-1210-52/ME:5# config lldp ports all dot1_tlv_vlan_name vlanid 1 disable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1 disable


Success.

DES-1210-52/ME:5#
```

config lldp ports

Purpose	To enable or disable LLDP management LLDP power pse TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] power_pse_tlv [enable | disable]**
Description	The **config lldp ports** dot1 TLVs command enable or disable the LLDP power pse TLVs per port on the switch.
Parameters	*[<portlist>* | *all]* – Specify a port or ports to be configured. *[enable* | *disable]* – Specify the LLDP power pse TLVS to be enable or disable for the specified port.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable LLDP power pse TLVs for port 3-5:

```
DES-1210-52/ME:5# config lldp ports 3-5 power_pse_tlv enable
Command: config lldp ports 3-5 power_pse_tlv enable


Success.

DES-1210-52/ME:5#
```

show lldp power_pse_tlv

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) power pse TLVs information.
Syntax	**show lldp power_pse_tlv**
Description	The **show lldp power_pse_tlv** command displays the information of power pse TLVs.
Parameters	None.
Restrictions	None.

Example usage:

To show the LLDP power pse TLVs:

```
DES-1210-52/ME:5# show lldp power_pse_tlv
Command: show lldp power_pse_tlv


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

show lldp mgt_addr

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) configuration that is advertised from a specific port.
Syntax	**show lldp mgt_addr {ipv4 <ipaddr> | ipv6 <ipv6addr>}**
Description	The **show lldp mgt_addr** command displays the information regarding the IPv4 or IPv6 address.
Parameters	*ipv4 <ipaddr>* | *ipv6 <ipv6addr>* **–** Specifies the lldp IPv4 or IPv6 address to be displayed.
Restrictions	None.

Example usage:

To show the LLDP management address advertisement:

```
DES-1210-52/ME:5# show lldp mgt_addr
Command: show lldp mgt_addr

Address : 1
---------------------------------------------------------------------------
   Subtype                          : IPv6
   Address                          : fe80::2c8:e7ff:fe88:5c95
   IF Type                          : ifIndex
   OID                              : 1.3.6.1.2.1.2.2.1.1
   Advertising Ports                : (NONE)


Total Address : 1

DES-1210-52/ME:5#
```

show lldp statistics

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) statistics for the specified ports.
Syntax	**show lldp statistics {ports <portlist>}**
Description	The **show lldp statistics** command displays the statistics of LLDP on the Switch.
Parameters	*{ports <portlist>* **–** Specifies the ports to be displayed.
Restrictions	None.

Example usage:

To show the LLDP statistics for port 15:

```
DES-1210-52/ME:5# show lldp statistics ports 15
Command: show lldp statistics ports 15

Port ID : 15
--------------------------------------------
lldpStatsTxPortFramesTotal                 : 0
lldpStatsRxPortFramesDiscardedTotal  : 0
lldpStatsRxPortFramesErrors               : 0
lldpStatsRxPortFramesTotal                 : 0
lldpStatsRxPortTLVsDiscardedTotal       : 0
lldpStatsRxPortTLVsUnrecognizedTotal : 0
lldpStatsRxPortAgeoutsTotal                 : 0

DES-1210-52/ME:5#
```

55

ACCESS CONTROL LIST COMMANDS

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

Command	Parameter
create access_profile	[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip { 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} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> } | protocol_id_mask <0x0-0xff>]} | packet_content_mask {offset1 [l2 | l3 | l4] <value (0-31)> <hex (0x0-0xffff)> | offset2 [l2 | l3 | l4] <value (0-31)> <hex (0x0-0xffff)>| offset3 [l2 | l3 | l4] <value (0-31)> <hex (0x0-0xffff)>| offset4 [l2 | l3 | l4] <value (0-31)> <hex (0x0-0xffff)>} | ipv6 { class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp { type | code }]} profile_id <value 1-10>]
config access_profile	profile_id <value (1-10)> [add access_id [auto_assign | <value 1-128>] [ethernet {vlan <vlanid (1-4094)> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value (0-7)> | ethernet_type <hex (0x0-0xffff)> } | ip {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)>]} | packet_content [offset1 <hex (0x0-0xffffffff)> | offset2 <hex (0x0-0xffffffff)> | offset3 <hex (0x0-0xffffffff)> | offset4 <hex (0x0-0xffffffff)>] | ipv6 [class <value 0-255> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr> | tcp [src_port < value 0-65535> | dst_port < value 0-65535>] | udp [src_port < value 0-65535> | dst_port < value 0-65535>] | icmp [type<value 0-255> | code <value 0-255>]] [port [<portlist> | all] [permit {replace_priority_with <value (0-7)> | replace_dscp_with <value (0-63)> | rx_rate {no_limit | <value (64-1024000)>}} | mirror | deny]] | delete access_id <value (1-128)>]
delete access_profile	profile_id <value 1-10>
show access_profile	{profile_id <value 1-10>}
create cpu_access_profile	[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {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} | udp {src_port_mask <hex (0x0-0xffff)> | dst_port_mask <hex (0x0-0xffff)>} | protocol_id_mask <hex (0x0-0xff)>]} | ipv6 {class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}] profile_id <value 1-3>
config cpu_access_profile	[profile_id <value (1-3)] [add access_id [auto_assign | <value (1-5)>]] [ethernet {vlan <vlanid (1-4094)> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value (0-7)> | ethernet_type <hex (0x0-0xffff)>} | ip {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)>] | ipv6 {class | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>} [port

Command	Parameter
	[<portlist> | all] [permit | deny]] delete access_id <value (1-5)>]
delete cpu_access_profile	profile_id <value 1-3>
enable cpu_interface_filtering	
disable cpu_interface_filtering	
show cpu_access_profile	{profile_id <value 1-3>}
config flow_meter profile_id	<value 1-10> access_id <value 1-128> [delete | rate <value 64-1024000>] burst_size <value 0-1016> rate_exceed [drop_packet | remark_dscp <value 0-63>]

Each command is listed in detail, as follows:

create access_profile	
Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create access_profile [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip { 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} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> } | protocol_id_mask <0x0-0xff>]} | packet_content_mask {offset1 [l2 | l3 | l4] <value (0-31)> <hex (0x0-0xffff)> | offset2 [l2 | l3 | l4] <value (0-31)> <hex (0x0-0xffff)>| offset3 [l2 | l3 | l4] <value (0-31)> <hex (0x0-0xffff)>| offset4 [l2 | l3 | l4] <value (0-31)> <hex (0x0-0xffff)>} | ipv6 { class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp { type | code }]} profile_id <value 1-10>]**
Description	The **create access_profile** command creates a profile for packets that may be accepted or denied 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 examines the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies that the Switch 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 examine the 802.1p priority value in the frame's header.
- *ethernet_type* – Specifies that the Switch examine the Ethernet type value in each frame's header.

ip - Specifies that the Switch examines the IP fields in each packet with special emphasis on one or more of the following:

icmp – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place.

- *type* – Specifies that the Switch examines each frame's ICMP Type field.
- *code* – Specifies that the Switch examines each frame's ICMP Code field.

igmp – Specifies that the Switch examine each frame's protocol field and it must be 2 (Internet Group Management Protocol-IGMP) for the action to take place.

- *type* – Specifies that the Switch examine each frame's IGMP Type field.

tcp – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place.

- *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* – Specifies the appropriate flag_mask parameter.

udp – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place..

- *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.

packet_content_mask – Specifies the frame content mask.

[offset1 | *offset2* | *offset3* | *offset4]* – Specifies the mask pattern offset of frame.

Ipv6 – Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following:

class – Examine the class field of the IPv6 header.

source_ipv6_mask <ipv6mask> – Specifies the IPv6 address mask for the source IP.

destination_ipv6_mask <ipv6mask> – Specifies the IPv6 address mask for the destination IP.

tcp – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place.

- *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. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place.. • *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. *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *type* – Specifies that the Switch examines each frame's ICMP Type field. • *code* – Specifies that the Switch examines each frame's ICMP Code field. *profile_id <value 1-10>* – Specifies an index number between 1 and 10 that identifies the access profile being created with this command.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an Ethernet access profile:

```
DES-1210-52/ME:5# create access_profile ethernet vlan 802.1p profile_id 1
Command: create access_profile ethernet vlan 802.1p profile_id 1

Success.
DES-1210-52/ME:5#
```

config access_profile

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are 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 ethernet** command, below.
Syntax	**config access_profile profile_id <value 1-10> [add access_id [auto_assign | <value 1-128>] [ethernet {vlan <vlanid 1-4094> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex (0x0-0xffff)> } | ip {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)>]} | packet_content [offset1 <hex (0x0-0xffffffff)> | offset2 <hex (0x0-0xffffffff)> | offset3 <hex (0x0-0xffffffff)> | offset4 <hex (0x0-0xffffffff)>] | ipv6 [class <value 0-255> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr> | tcp [src_port < value 0-65535> | dst_port < value 0-65535>] | udp [src_port < value 0-65535> | dst_port < value 0-65535>] | icmp [type<value 0-255> | code <value 0-255>]] [port [<portlist> | all] [permit {replace_priority_with <value (0-7)> | replace_dscp_with <value (0-63)> | rx_rate {no_limit | <value (64-1024000)>}} | mirror |**

deny]] | delete access_id <value (1-128)>]

Description

The **config access_profile ethernet** command defines the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.

Parameters

profile_id <value 1-10> – Specifies the access profile id to 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 | delete] access_id <value 1-65535> – Adds or deletes an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 65535 rules may be configured for the Ethernet access profile.

- *auto_assign* – Configures the Switch to automatically assign a numerical value (between 1 and 65535) for the rule being configured.

ethernet – Specifies that the Switch examine only 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 <vlanid 1-4094>* – Specifies that the access profile applies only to this previously created VLAN.
- *source_mac <macaddr>* – Specifies that the access profile applies only to 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 applies only to 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 applies only to packets with this 802.1p priority value.
- *ethernet_type <hex 0x05dd-0xffff>* – Specifies that the access profile applies only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

ports <portlist> **-** The access profile for Ethernet may be defined for each port on the Switch.

- *mirror* – Specifies the action to mirror before being forwarded by the Switch.
- *replace_dscp_with <value 0-63>* – Specifies 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.
- *rx_rate <value 64-1024000>* – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.

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

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

- *source_ip <ipaddr>* – Specifies that the access profile applies only to packets with this source IP address.
- *protocol_id <value 0-255>* – Specifies that the Switch examine the Protocol field in each packet and if this field contains the value entered here, apply the appropriate rules.
- *destination_ip <ipaddr>* – Specifies that the access profile applies only to packets with this destination IP address.
- *dscp <value 0-63>* – Specifies that the access profile applies 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 examine the protocol field in each frame's header and it should match Internet Control Message Protocol (ICMP).
- *type* – Specifies that the Switch examine each frame's ICMP Type field.
- *code* – Specifies that the Switch examine each frame's ICMP Code field.
- *igmp* – Specifies that the Switch examine each frame's protocol and it should match Internet Group Management Protocol (IGMP) field.
- *type* – Specifies that the Switch examine each frame's IGMP Type field.
- *tcp* - Specifies that the Switch examine each frame's protocol and it should matchTransport Control Protocol (TCP) field.
- *src_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this TCP source port in their TCP header.
- *dst_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this TCP destination port in their TCP header.
- *flag {+ | –} {urg | ack | psh | rst | syn | fin }}* – Specifies the appropriate flag parameter. All incoming packets have TCP 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.

  To specify flag bits that should be "1" type + and the flag bit name, to specify bits that should be "0" type – and the flag bit name.
- *udp* – Specifies that the Switch examine the protocol field in each packet and it should match User Datagram Protocol (UDP).
- *src_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this UDP source port in their header.
- *dst_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this UDP destination port in their header.

Ipv6 – Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following:

class <value 0-255> – Examine the class field of IPv6 header. The range is 0 to 255.

	source_ipv6 <ipv6addr> – Specifies that the access profile applies only to packets with this source IPv6 address. *destination_ipv6 <ipv6addr>* – Specifies that the access profile applies only to packets with this destination IPv6 address. *tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place. • *src_port <value 0-65535>* – Specifies the TCP source port range. The range is between 0 and 65535. • *dst_port <value 0-65535>* – Specifies the TCP destination port range. The range is between 0 and 65535. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *src_port <value 0-65535>* –Specifies the UDP source port range. The range is between 0 and 65535. • *dst_port <value 0-65535>* –Specifies the UDP destination port range. The range is between 0 and 65535. *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *type <value 0-255>* – Specifies that the Switch examines each frame's ICMP Type field. The range is between 0 and 255. • *code <value 0-255>* – Specifies that the Switch examines each frame's ICMP Code field. The range is between 0 and 255. *port [<portlist>* | *all*| - The access profile for IP may be defined for each port on the Switch. *permit* – Specifies that packets that match the access profile are permitted to be forwarded by the Switch. • *mirror* – Specifies the action to mirror before being forwarded by the Switch. • *replace_dscp_with <value 0-63>* – Specifies 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. *rx_rate <value 64-1024000>* – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the Ethernet access profile:

```
DES-1210-52/ME:5# config access_profile profile_id 2 add access_id 2 ip
protocol_id 2 ports 2 deny
Command: config access_profile profile_id 2 add access_id 2 ip protocol_id
```

```
 2 ports 2 deny

Success.

DES-1210-52/ME:5#
```

delete access_profile

Purpose	To delete a previously created access profile
Syntax	**delete access_profile profile_id <value 1-10>**
Description	The **delete access_profile** command deletes a previously created access profile on the Switch.
Parameters	*profile_id <value 1-10>* – Specifies the access profile to be deleted.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

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

```
DES-1210-52/ME:5# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DES-1210-52/ME:5#
```

show access_profile

Purpose	To display the currently configured access profiles on the Switch.
Syntax	**show access_profile {profile_id <value 1-10>}**
Description	The **show access_profile** command displays the currently configured access profiles.
Parameters	*profile_id <value 1-10>* – Specifies the access profile to be displayed. This value is assigned to the access profile when it is created with the **create access_profile** command. If the *profile_id* parameter is omitted, all access profile entries are displayed.
Restrictions	None.

Example usage:

To display the currently configured access profiles which profile id is 1 on the Switch:

```
DES-1210-52/ME:5# show access_profile profile_id 1
Command: show access_profile profile_id 1


Access Profile Table

Access Profile ID: 1          Type: Ethernet
---------------------------------------------------------------------------
---------------------------------------------------------------------------
Mask Option:
VLAN   802.1p
---------------------------------------------------------------------------


DES-1210-52/ME:5#
```

create cpu_access_profile

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are 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 cpu_access_profile [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {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} | udp {src_port_mask <hex (0x0-0xffff)> | dst_port_mask <hex (0x0-0xffff)>} | protocol_id_mask <hex (0x0-0xff)>]} | ipv6 {class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}] profile_id <value 1-3>**
Description	The **create cpu_access_profile** command is used to create CPU access list rules on the Switch.
Parameters	*ethernet* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies a VLAN mask. • *source_mac <macmask >* – Specifies the source MAC mask. • *destination_mac <macmask>* – Specifies the destination MAC mask. • *802.1p* – Specifies 802.1p priority tag mask. *ethernet_type* – Specifies the Ethernet type mask. *ip* - Specifies that the Switch examines the IP fields in each packet with special emphasis on one or more of the following: • *type* – Specifies that the Switch examine each frame's ICMP Type field. • *code* – Specifies that the Switch examine each frame's ICMP code field. • *type* – Specifies that the Switch examine each frame's IGMP

	Type field. *tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place. • *src_port_mask <hex 0x0-0xffff>* – Specifies the TCP port mask for the source port. • *dst_port_mask <hex 0x0-0xffff>* – Specifies the TCP port mask for the destination port. • flag_mask - Specifies the appropriate flag. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *src_port_mask <0x0-0xffff>* – Specifies the UDP port mask for the source port. • *dst_port_mask <0x0-0xffff>* – Specifies the UDP port mask for the destination port mask. • *protocol_id_mask <0x0-0xffff>* – Specifies the protocol id mask. • *source_ip_mask <netmask>* – Specifies the source IPv4 mask. • *destination_ip_mask <netmask>* – Specifies the destination IPv4 mask. *dscp* – Specifies that the Switch examines the DiffServ Code Point (DSCP) field in each frame's header. *ipv6* - Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following: • *class* – Examine the class field of the IPv6 header. • *source_ipv6_mask <ipv6mask>* – Specifies the source IPv6 mask. • *destination_ipv6_mask < ipv6mask >* – Specifies the destination IPv6 mask. *profile_id <value 1-3>* – Specifies the cpu access profile to be displayed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create a CPU IP access profile:

```
DES-1210-52/ME:5# create cpu access_profile ip source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2
Command: create cpu access_profile ip source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2


Success.
DES-1210-52/ME:5#
```

config cpu_access_profile

Purpose	To configures the settings of cpu access profiles.
Syntax	**config cpu_access_profile [profile_id <value (1-3)] [add access_id [auto_assign | <value (1-5)>]] [ethernet {vlan <vlanid (1-4094)> | source_mac <macaddr> | destination_mac**

<macaddr> | 802.1p <value (0-7)> | ethernet_type <hex (0x0-0xffff)>} | ip {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)>] | ipv6 {class | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>} [port [<portlist> | all] [permit | deny]] delete access_id <value (1-5)>]

Description

The **config cpu_access_profile** command configures the settings of cpu access profiles.

Parameters

profile_id <value 1-3> – Specifies the cpu access profile to be configured.

[add | *delete]* – Add or delete the profile id.
access_id [<value 1-5> | *auto_assign]* – Specifies the access id value or use auto assign.
ethernet – Specifies that the Switch examine only 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:

- *802.1p <value 0-7>* – Specifies the 802.1p value. The range is between 0 and 7.
- *destination_mac <macaddrf>* – Specifies the destination MAC address.
- *ethernet_type* – Specifies the Ethernet type mask.
- *<portlist>* – Specifies the port or ports to be configured.
- *source_mac <macaddr>* – Specifies the source MAC address.

vlan <vlanid 1-4094> – Specifies the VLAN id.

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

- *destination_ip <ip_addr>* – Specifies the destination IP address.
- *dscp <value 0-63>* – Specifies the DSCP value.

icmp – Specifies that the Switch examines the Protocol field in each frame’s IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place.

- *code <value 0-255>* –Specifies that the Switch examine each frame’s ICMP code field.
- *type <value 0-255>* –Specifies that the Switch examine each frame’s ICMP Type field.

igmp – Specifies that the Switch examine each frame’s protocol field and it must be 2 (Internet Group Management Protocol-IGMP) for the action to take place.

- *igmp_type <value 0-255>* – Specifies the IGMP type.

<portlist> – Specifies the port or ports to be configured.

protocol_id <value 0-255> – Specifies the protocol id.

source_ip <ip_addr> –Specifies that the cpu access profile applies only to packets with this source IP address.

Tcp – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place

- *dst_port <value 0-65535>* –Specifies that the cpu access

	profile applies only to packets that have this TCP destination port in their header. • *flag <string>* – Specifies the appropriate flag parameter. • *src_port <value 0-65535>* –Specifies that the cpu access profile applies only to packets that have this TCP source port in their header. *udp* – Specifies that the Switch examines each frame’s protocol field and it’s value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *dst_port <value 0-65535>* – Specifies that the CPU access profile applies only to packets that have this UDP destination port in their header. *src_port <value 0-65535>* – Specifies that the CPU access profile applies only to packets that have this UDP source port in their header. *ipv6* - Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following: • *class* – Examine the class field of the IPv6 header. • *source_ipv6 <ipv6addr>* – Specifies the source IPv6 address. • *destination_ipv6 < ipv6addr >* – Specifies the destination IPv6 address.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the CPU IP access profile:

```
DES-1210-52/ME:5# config cpu access_profile profile_id 2 add access_id
auto_assignip destination_ip 10.48.100.2 ports 1-3 permit
Command: config cpu access_profile profile_id 2 add access_id auto_assign
ip destination_ip 10.48.100.2 ports 1-3 permit

Success.

DES-1210-52/ME:5#
```

delete cpu_access_profile

Purpose	To delete a previously created cpu access profile.
Syntax	**delete cpu_access_profile profile_id <value 1-3>**
Description	The **delete cpu_access_profile** command deletes a previously created access profile on the Switch.
Parameters	*profile_id <value 1-3>* – Specifies the cpu access profile to be deleted.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

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

```
DES-1210-52/ME:5# delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DES-1210-52/ME:5#
```

enable cpu_interface_filtering

Purpose	To enable CPU interface filtering on the Switch.
Syntax	**enable cpu_interface_filtering**
Description	The **enable cpu_interface_filtering** command is used to enable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To enable the CPU filtering on the Switch:

```
DES-1210-52/ME:5# enable cpu_interface_filtering
Command: enable cpu_interface_filtering


Success.
DES-1210-52/ME:5#
```

disable cpu_interface_filtering

Purpose	To disable CPU interface filtering on the Switch.
Syntax	**disable cpu_interface_filtering**
Description	The **disable cpu_interface_filtering** command is used to disable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To disable the CPU filtering on the Switch:

```
DES-1210-52/ME:5# disable cpu_interface_filtering
Command: disable cpu_interface_filtering


Success.
DES-1210-52/ME:5#
```

show cpu_access_profile

Purpose	To view the CPU access profile entry currently set in the Switch.
Syntax	**show cpu_access_profile {profile_id <value 1-3>}**
Description	The **show cpu access_profile** command is used view the current CPU interface filtering entries set on the Switch.
Parameters	*profile_id <value 1-3>* – Enter an integer between 1 and 3 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	None.

Example usage:

To show the CPU filtering state on the Switch:

```
DES-1210-52/ME:5# show cpu_access_profile
Command: show cpu_access_profile



Access Profile Table

Access Profile ID: 1          Type: Ethernet
--------------------------------------------------------------------------
--------------------------------------------------------------------------
Mask Option:
VLAN
-------------------------------------------------------------------------
DES-1210-52/ME:5#
```

config flow_meter profile_id

Purpose	To configure the flow-based metering function on the Switch.
Syntax	**config flow_meter profile_id <value 1-10> access_id <value 1-128> [delete | rate <value 64-1024000>] burst_size <value 0-1016> rate_exceed [drop_packet | remark_dscp <value 0-63>]**
Description	The **config flow_meter profile_id** command configures the flow-based metering function on the Switch.
Parameters	*profile_id <value 1-10>* - .Specify the profile id to be configured. *access_id <value 1-128>* - Specify the access id to be configured. *rate <value 64-1024000>* - Specifies the committed bandwidth in Kbps for the flow. *burst_size <value 0-1016>* - Specifies the burst size *rate_exceed:* pecifies the action for packets that exceeds the committed rate in single rate *drop_packet* - Drop the packet immediately. *remark_dscp <value 0-63>* - Specify the remark DSCP value.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To config flow meter information:

```
DES-1210-52/ME:5# config flow_meter profile_id 1 access_id 1 rate 64
burst_size 10 rate_exceed remark_dscp 2
Command: config flow_meter profile_id 1 access_id 1 rate 64
burst_size 10 rate_e
xceed remark_dscp 2
```

56

TRAFFIC SEGMENTATION COMMANDS

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

Command	Parameter
config traffic_segmentation	<portlist> forward_list [null | <portlist>]
show traffic_ segmentation	{<portlist>}

Each command is listed in detail, as follows:

config traffic_segmentation	
Purpose	To configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation <portlist> forward_list [null | <portlist>]**
Description	The **config traffic_segmentation** command configures traffic segmentation on the Switch.
Parameters	*<portlist>* – A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed. *forward_list* – Specifies a port or a port channel to receive forwarded frames from the source ports specified in the portlist, above.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure ports 1~5 to be able to forward frames to port 5~8:

```
DES-1210-52/ME:5# config traffic_segmentation 1-5 forward_list 5-8
Command: config traffic_segmentation 1-5 forward_list 5-8

Success.

DES-1210-52/ME:5#
```

show traffic_segmentation	
Purpose	To display the current traffic segmentation configuration on the Switch.
Syntax	**show traffic_segmentation {<portlist>}**
Description	The **show traffic_segmentation** command displays the current traffic segmentation configuration on the Switch.
Parameters	*<portlist>* – A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed.

Restrictions	None.

Example usage:

To display the current traffic segmentation configuration of ports 1 to 3 on the Switch:

```
DES-1210-52/ME:5# show traffic_segmentation 1-3
Command: show traffic_segmentation 1-3


Port  Forward Portlist
----  -------------------------------------------------
1     3-5
2     3-5
3     3-5
DES-1210-52/ME:5#
```

57

SAFEGUARD COMMANDS

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

Command	Parameter
config safeguard_engine	state [enable | disable]
show safeguard_engine	

Each command is listed in detail, as follows:

config safeguard_engine

Purpose	To define the safeguard engine on the switch.
Syntax	**config safeguard_engine state [enable | disable]**
Description	To define the safeguard_engine on the switch.
Parameters	*state [enable* | *disable]* – enable and disable Safeguard engine on the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the safeguard engine on the switch:

```
DES-1210-52/ME:5# config safeguard_engine state enable
Command: config safeguard_engine state enable



Success.
DES-1210-52/ME:5#
```

show safeguard_engine

Purpose	To show the safeguard engine status on the switch.
Syntax	**show safeguard_engine**
Description	To show the safeguard engine on the switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To show the safeguard engine status on the switch:

```
DES-1210-52/ME:5# show safeguard_engine
Command: show safeguard_engine


Safe Guard : Enabled
DES-1210-52/ME:5#
```

58

DEVICE SPECIFICATIONS

This appendix contains the device specifications, and contains the following topics:

- Technical Specifications
- Supported Transceivers

Technical Specifications

Performance	
Transmission Method	Store-and-forward
SDRAM for CPU	256M DDR3
Switching Capacity	17.6Gps
Packet Filtering/ Forwarding Rate	13.1 million packets per second
Packet Buffer	12Mbits
MAC Address Learning	Automatic update. Supports 16K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10–600 seconds. Default = 300.

Physical and Environmental	
AC Inputs	20W AC Input: 100 – 240 VAC, 50-60 Hz
Power Consumption	Maximum power consumption: 14.52Watts Standby power consumption: 7.08Watts
DC Fans	Fanless
Operating Temperature	-5 to 50 degrees Celsius
Storage Temperature	-40 to 70 degrees Celsius
Humidity	Storage: 5% to 90% non-condensing
Dimensions	19-inch, 1U Rack-mount size: 440 mm x 210 mm x 44 mm
Weight	2.85kg
EMI Certifications	FCC, CE, C-Tick, VCCI, BSMI, CCC
Safety Certifications	cUL, LVD, CB, CE, CCC, BSMI

General		
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z Gigabit Ethernet IEEE 802.1Q Tagged VLAN IEEE 802.1P Tagged Packets IEEE 802.3ab 1000BASE-T IEEE 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 NWay auto-negotiation	
Protocols	CSMA/CD	
Data Transfer Rates	Half-duplex	Full-duplex
Ethernet:	10 Mbps	20 Mbps
Fast Ethernet:	100 Mbps	200 Mbps
Gigabit Ethernet:	2000 Mbps (Full duplex only)	
Topology	Star	

Network Cables	
10BASE-T:	UTP Category 3, 4, 5 (100 meters max.) EIA/TIA- 568 150-ohm STP (100 meters max.)
100BASE-TX:	UTP Cat. 5 (100 meters max.) EIA/TIA-568 150-ohm STP (100 meters max.)
1000BASE-T:	UTP Cat. 5e (100 meters max.) UTP Cat. 5 (100 meters max.) EIA/TIA-568B 150-ohm STP (100 meters max.)
Number of Ports:	48 x 10/100 Mbps ports 4 x combo 10/100/1000Based-T/100/1000 SFP

Supported Transceivers

Supported SFP Transceivers:

Module	Description	Maximum Distance
DEM-210	SFP Transceiver for 100BASE-FX, Single-mode fiber module	15km
DEM-211	SFP Transceiver for 100BASE-FX, Multi-mode fiber module	2km
DEM-310GT	SFP Transceiver for 1000BASE-LX, Single-mode fiber module	10km
DEM-311GT	SFP Transceiver for 1000BASE-SX, Multi-mode fiber module	550m
DEM-312GT2	SFP Transceiver for 1000BASE-SX, Multi-mode fiber module	2km
DEM-314GT	SFP Transceiver for 1000BASE-LHX, Single-mode fiber module	50km
DEM-315GT	SFP Transceiver for 1000BASE-ZX, Single-mode fiber module	80km
DGS-712	1000BASE-T (only support 1000Mbps mode – no flow control)	100m
DEM-302LX	1000BASE-LX, Single mode	2km

Supported WDM Transceivers:

Module	Description	Maximum Distance
DEM-220R	WDM Transceiver for 100BASE-FX WDM transceiver, Single-mode fiber module	20km
DEM-220T	WDM Transceiver for 100BASE-FX WDM transceiver, Single-mode fiber module	20km
DEM-330T/R	WDM Transceiver for Gigabit WDM transceiver, Single-mode fiber module	10km
DEM-331T/R	WDM Transceiver for Gigabit WDM transceiver, Single-mode fiber module	40km
DEM-302S-BXD/BXU	WDM Transceiver for Gigabit WDM transceiver, Single-mode fiber module	2km
DEM-320S-BXD	WDM Transceiver for Gigabit WDM transceiver, Single-mode fiber module	2km