



# CLI Reference Manual

Product Model : DES-1228/ME

Managed 10/100Mbps Metro Ethernet Switch

Release 1

---

Information in this document is subject to change without notice.

© 2009 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

August 2009 P/N 651ES1228015G

# Table of Contents

---

<b>INTRODUCTION .....</b>	<b>1</b>
<b>USING THE CONSOLE CLI.....</b>	<b>3</b>
<b>COMMAND SYNTAX .....</b>	<b>7</b>
<b>BASIC SWITCH COMMANDS.....</b>	<b>9</b>
<b>MODIFY BANNER AND PROMPT COMMANDS .....</b>	<b>21</b>
<b>SWITCH PORT COMMANDS .....</b>	<b>24</b>
<b>PORT SECURITY COMMANDS .....</b>	<b>28</b>
<b>NETWORK MANAGEMENT (SNMP) COMMANDS .....</b>	<b>32</b>
<b>SWITCH UTILITY COMMANDS .....</b>	<b>54</b>
<b>NETWORK MONITORING COMMANDS .....</b>	<b>64</b>
<b>MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS .....</b>	<b>76</b>
<b>FORWARDING DATABASE COMMANDS .....</b>	<b>88</b>
<b>BROADCAST STORM CONTROL COMMANDS .....</b>	<b>98</b>
<b>COS COMMANDS .....</b>	<b>101</b>
<b>PORT MIRRORING COMMANDS .....</b>	<b>116</b>
<b>VLAN COMMANDS .....</b>	<b>119</b>
<b>LINK AGGREGATION COMMANDS.....</b>	<b>126</b>
<b>BASIC IP COMMANDS.....</b>	<b>131</b>
<b>IGMP SNOOPING COMMANDS.....</b>	<b>134</b>
<b>DHCP RELAY.....</b>	<b>144</b>
<b>802.1X COMMANDS .....</b>	<b>151</b>
<b>ACCESS CONTROL LIST (ACL) COMMANDS.....</b>	<b>170</b>

<b>SAFEGUARD ENGINE COMMANDS .....</b>	<b>182</b>
<b>TRAFFIC SEGMENTATION COMMANDS.....</b>	<b>184</b>
<b>TIME AND SNTP COMMANDS .....</b>	<b>186</b>
<b>ARP COMMANDS.....</b>	<b>192</b>
<b>ROUTING TABLE COMMANDS.....</b>	<b>196</b>
<b>MAC NOTIFICATION COMMANDS .....</b>	<b>198</b>
<b>ACCESS AUTHENTICATION CONTROL COMMANDS .....</b>	<b>202</b>
<b>SSH COMMANDS .....</b>	<b>222</b>
<b>SMTP COMMANDS .....</b>	<b>229</b>
<b>CABLE DIAGNOSTICS COMMANDS.....</b>	<b>233</b>
<b>DHCP LOCAL RELAY COMMANDS .....</b>	<b>234</b>
<b>GRATUITOUS ARP COMMANDS.....</b>	<b>236</b>
<b>VLAN TRUNKING COMMANDS .....</b>	<b>240</b>
<b>ASYMMETRIC VLAN COMMANDS .....</b>	<b>244</b>
<b>IGMP SNOOPING MULTICAST VLAN COMMANDS.....</b>	<b>246</b>
<b>LLDP COMMANDS .....</b>	<b>251</b>
<b>PPPOE COMMANDS.....</b>	<b>270</b>
<b>IP-MAC-PORT BINDING COMMANDS.....</b>	<b>273</b>
<b>LAYER 3 CONTROL PACKET FILTERING.....</b>	<b>278</b>
<b>LOOPBACK DETECTION COMMANDS.....</b>	<b>280</b>
<b>TECHNICAL SUPPORT COMMANDS.....</b>	<b>284</b>
<b>COMMAND HISTORY LIST.....</b>	<b>287</b>
<b>DHCP SERVER SCREEN LIST .....</b>	<b>292</b>

**ARP SPOOFING ATTACK PREVENTION LIST .....295**

**TECHNICAL SPECIFICATIONS.....297**

## INTRODUCTION

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

This manual provides a reference for all of the commands contained in the CLI. Configuration and management of the Switch via the Web-based management agent is discussed in the Manual. This manual provides a reference for all of the commands contained in the CLI for members of this series, including the DES-1228/ME. Examples present in this manual may refer to any member of this series and may show different port counts, but are universal to this series of switches, unless otherwise stated. Configuration and management of the Switch via the Web-based management agent is discussed in the User's Guide.

### Accessing the Switch via the Serial Port

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

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

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

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

```
DES-1228/ME Metro Ethernet Switch Command Line Interface
Firmware: Build 1.00.B04
Copyright(C) 2009 D-Link Corporation. All rights reserved.

username:
```

**Figure 1-1. Initial CLI screen**

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-1228/ME:4#**. This is the command line where all commands are input.

## Setting the Switch's IP Address

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

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

```

Boot Procedure V1.00.01
-----
Power On Self Test.....100%
MAC Address : 00-21-91-98-60-77
H/W Version : A1
Please wait, loading V1.00.B04 Runtime image.....100%

```

**Figure 1-2. Boot screen**

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

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

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

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

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

```

DES-1228/ME:4#config ipif System ipaddress 10.73.21.11/255.0.0.0
Command: config ipif System ipaddress 10.73.21.11/8
Success.

DES-1228/ME:4#

```

**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 successfully. The Switch can now be configured and managed via Telnet, SNMP MIB browser and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

## USING THE CONSOLE CLI

The DES-1228/ME support a console management interface that allows the user to connect to the Switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the Switch to use an SNMP-based network management software over the network.

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



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

### Connecting to the Switch

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

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

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

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

```
DES-1228/ME Metro Ethernet Switch Command Line Interface
Firmware: Build 1.00.B04
Copyright(C) 2009 D-Link Corporation. All rights reserved.

username :
```

**Figure 2-1. Initial Console Screen after logging in**

Commands are entered at the command prompt, **DES-1228/ME:4#**.

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



```

.
?
cable_diag ports
clear
clear arptable
clear counters
clear fdb
clear flood_fdb
clear igmp_snooping data_driven_group
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account

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

```

**Figure 2-2. The ? Command**

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

```

DES-1228/ME:4#config account
Command: config account

Next possible completions:
<username>

DES-1228/ME:4#

```

**Figure 2-3. Example Command Parameter Help**

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

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

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

```

DES-1228/ME:4#config account
Command: config account

Next possible completions:
<username>

DES-1228/ME:4#config account
Command: config account

Next possible completions:
<username>

DES-1228/ME:4#

```

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

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

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

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

```

DES-1228/ME:4#the

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

DES-1228/ME:4#

```

**Figure 2-5. The Next Available Commands Prompt**

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

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

```

DES-1228/ME:4#show
Command: show

Next possible completions:
802.1p          802.1x          access_profile  account
acct_client     address_binding arp_spoofing_prevention
arpentry        asymmetric_vlan auth_client      auth_diagnostics
auth_session_statistics
authen_enable   authen_login    auth_statistics  authen
autoconfig      bandwidth_control
command         command_history
config          cos             cpu_access_profile
cpu_filter      dhcp_local_relay
error          fdb             dhcp_relay       dscp_mapping
flood_fdb      gratuitous_arp  filter           firmware
igmp_snooping  ipif            greeting_message gvrp
link_aggregation
lldp            lldp            log              log_save_timing
loopdetect     mac_notification
multicast      multicast_fdb   mgmt_pkt_priority mirror
ports          mlticast_fdb   packet           port_security
safeguard_engine
serial_port     session         radius           router_ports
snmp           ssh             scheduling_mechanism
syslog         tech_support    smtp            snmp
traffic        traffic_segmentation
utilization     vlan            stp             switch
               vlan_trunk     stp             switch
               terminal_line  stp             switch
               time
               trusted_host
DES-1228/ME:4#

```

**Figure 2-6. Next possible completions: Show Command**

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

## COMMAND SYNTAX

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual.



**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	<b>config ipif &lt;ipif_name 12&gt; [{ipaddress &lt;network_address&gt;   vlan &lt;vlan_name 32&gt;   state [enable   disable]}]   bootp   dhcp]</b>
Description	In the above syntax example, users must supply an IP interface name in the <ipif_name 12> space, a VLAN name in the <vlan_name 32> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	<b>config ipif System ipaddress 10.24.22.5/255.0.0.0 vlan default state enable</b>

### [square brackets]

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

### | vertical bar

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

### {braces}

Purpose	Encloses an optional value or set of optional arguments.
Syntax	<b>reset {[config   system]}</b>
Description	In the above syntax example, users have the option to specify <b>config</b> or <b>system</b> . It is not necessary to specify either optional value, however the effect of the system reset is dependent on which, if any, value is specified. Therefore, with this example there are three possible outcomes of performing a system reset. See the following chapter, Basic Commands for more details about the reset command.
Example command	<b>reset config</b>

**(parentheses)**

Purpose	Indicates at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified.
Syntax	<b>config dhcp_relay {hops &lt;value 1-16&gt;   time &lt;sec 0-65535&gt;}(1)</b>
Description	In the above syntax example, users have the option to specify <b>hops</b> or <b>time</b> or both of them. The "(1)" following the set of braces indicates at least one argument or value within the braces must be specified. Do not type the parentheses.
Example command	<b>config dhcp_relay hops 3</b>

**Line Editing Key Usage**

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

**Multiple Page Display Control Keys**

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

## BASIC SWITCH COMMANDS

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

Command	Parameters
enable password encryption	
disable password encryption	
create account	[admin   user] <username 15>
config account	<username 15>
show account	
delete account	<username 15>
show session	
show switch	
show serial_port	
config serial_port	{ baud_rate [9600 19200 38400 115200]   auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes] }(1)
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
telnet	<ipaddr> {tcp_port <value 0-65535>}
enable web	<tcp_port_number 1-65535>
disable web	
save	{[config {config_id <value 1-2>}   log   all]}
reboot	{force_agree}
reset	{[config   system ]} { force_agree}
login	
logout	

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

## enable password encryption

Purpose	Used to enable password encryption on a user account.
Syntax	<b>enable password encryption</b>
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-1228/ME:4#enable password encryption
Command: enable password encryption

Success.

DES-1228/ME:4#
```

## disable password encryption

Purpose	Used to disable password encryption on a user account.
Syntax	<b>disable password encryption</b>
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 disable password encryption on the Switch.

```
DES-1228/ME:4#disable password encryption
Command: disable password encryption

Success.

DES-1228/ME:4#
```

## create account

Purpose	Used to create user accounts.
Syntax	<b>create account [admin   user] &lt;username 15&gt;</b>
Description	The <b>create account</b> command is used to create user accounts that consist of a username of 1 to 15 characters and a password of 0 to 15 characters. Up to 8 user accounts can be created.
Parameters	<i>admin &lt;username&gt;</i> <i>user &lt;username&gt;</i>
Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.

Example usage:

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

```
DES-1228/ME:4#create account admin dlink
Command: create account admin dlink

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

Success.

DES-1228/ME:4#
```

## config account

Purpose	Used to configure user accounts
Syntax	<b>config account &lt;username&gt;</b>
Description	The <b>config account</b> command configures a user account that has been created using the <b>create account</b> command.
Parameters	<i>&lt;username&gt;</i>
Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 35 characters.

Example usage:

To configure the user password of “dlink” account:

```
DES-1228/ME:4#config account dlink
Command: config account dlink

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

Success.

DES-1228/ME:4#
```



## show account

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

Example usage:

To display the accounts that have been created:

```
DES-1228/ME:4#show account
```

```
Command: show account
```

```
Current Accounts:
```

```
Username          Access Level
-----          -
dlink              Admin
```

```
Total Entries: 1
```

```
DES-1228/ME:4#
```

## delete account

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

Example usage:

To delete the user account "System":

```
DES-1228/ME:4#delete account System
```

```
Command: delete account System
```

```
Success.
```

```
DES-1228/ME:4#
```

## show session

Purpose	Used to display a list of currently logged-in users.
Syntax	<b>show session</b>
Description	This command displays a list of all the users that are logged-in at the time the command is issued.
Parameters	None.
Restrictions	None.

Example usage:

To display the way that the users logged in:

```
DES-1228/ME:4#show session
Command: show session

ID      Login Time                Live Time                From                    Level    Name
--      -
8       00000 days 00:00:37      0:3:36:27              Serial Port             4          Anonymous

Total Entries: 1

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

## show switch

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

Example usage:

To display the Switch's information:

```
DES-1228/ME:4#show switch
Command: show switch

Device Type       : DES-1228/ME Metro Ethernet Switch
MAC Address       : 00-19-5B-EF-78-B5
IP Address        : 10.73.21.11 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.B01
Firmware Version  : Build 1.00.B04
Hardware Version  : A1
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
VLAN trunk        : Disabled
802.1x            : Disabled
TELNET            : Enabled(TCP 23)
WEB               : Enabled(TCP 80)
RMON              : Disabled
SSH               : Disabled
Clipaging         : Enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## show serial\_port

Purpose	Used to display the current serial port settings.
Syntax	<b>show serial_port</b>
Description	This command displays the current serial port settings.
Parameters	None.
Restrictions	None

Example usage:

To display the serial port setting:

```
DES-1228/ME:4#show serial_port
Command: show serial_port

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

DES-1228/ME:4#
```

## config serial\_port

Purpose	Used to configure the serial port.
Syntax	<b>config serial_port { baud_rate [9600 19200 38400 115200]   auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes] }(1)</b>
Description	This command is used to configure the serial port's baud rate and auto logout settings.
Parameters	<p><i>baud_rate [9600   19200   38400   115200]</i> – The serial bit rate that will be used to communicate with the management host. There are four options: 9600, 19200, 38400, 115200.</p> <p><i>never</i> – No time limit on the length of time the console can be open with no user input.</p> <p><i>2_minutes</i> – The console will log out the current user if there is no user input for 2 minutes.</p> <p><i>5_minutes</i> – The console will log out the current user if there is no user input for 5 minutes.</p> <p><i>10_minutes</i> – The console will log out the current user if there is no user input for 10 minutes.</p> <p><i>15_minutes</i> – The console will log out the current user if there is no user input for 15 minutes.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the baud rate:

```
DES-1228/ME:4#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

DES-1228/ME:4#
```

## enable clipaging

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

Example usage:

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

```
DES-1228/ME:4#enable clipaging
Command: enable clipaging

Success.

DES-1228/ME:4#
```

## disable clipaging

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

Example usage:

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

```
DES-1228/ME:4#disable clipaging
Command: disable clipaging

Success.

DES-1228/ME:4#
```

## enable telnet

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

Example usage:

To enable Telnet and configure port number:

```
DES-1228/ME:4#enable telnet 23
```

```
Command: enable telnet 23
```

```
Success.
```

```
DES-1228/ME:4#
```

## disable telnet

Purpose	Used to disable the Telnet protocol on the Switch.
Syntax	<b>disable telnet</b>
Description	This command is used to disable the Telnet protocol on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the Telnet protocol on the Switch:

```
DES-1228/ME:4#disable telnet
```

```
Command: disable telnet
```

```
Success.
```

```
DES-1228/ME:4#
```

## telnet

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

Example usage:

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

```
DES-1228/ME:4#telnet 10.53.13.99 tcp_port 23
```

```
Command: telnet 10.53.13.99 tcp_port 23
```

## enable web

Purpose	Used to enable the HTTP-based management software on the Switch.
Syntax	<b>enable web &lt;tcp_port_number 1-65535&gt;</b>
Description	This command is used to enable the Web-based management software on the Switch.
Parameters	<tcp_port_number 1-65535> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” port for the Web-based management software is 80.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DES-1228/ME:4#enable web 80
```

```
Command: enable web 80
```

```
Success.
```

```
DES-1228/ME:4#
```

## disable web

Purpose	Used to disable the HTTP-based management software on the Switch.
Syntax	<b>disable web</b>
Description	This command disables the Web-based management software on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable HTTP:

```
DES-1228/ME:4#disable web
```

```
Command: disable web
```

```
Success.
```

```
DES-1228/ME:4#
```

## save

Purpose	Used to save changes in the Switch’s configuration to non-volatile RAM.
Syntax	<b>save {[config {config_id &lt;value 1-2&gt;}   log   all]}</b>
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the Switch’s memory each time the Switch is restarted.
Parameters	<i>config</i> – Used to save the current configuration to a file. <i>log</i> – Used to save the current log to a file. The log file cannot be deleted. <i>all</i> – Save changes to currently activated configurations and save log. If no keywords are specified, save the changes to the configuration. If there are no keywords specified, the changes will be saved to the configuration.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#save
Command: save

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

Success.

DES-1228/ME:4#
```

## reboot

Purpose	Used to restart the Switch.
Syntax	<b>reboot</b>
Description	This command is used to restart the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To restart the Switch:

```
DES-1228/ME:4#reboot
Command: reboot
Are users sure want to proceed with the system reboot? (y|n)
Please wait, the switch is rebooting...
```

## reboot force\_agree

Purpose	Used to force the Switch to restart.
Syntax	<b>reboot force_agree</b>
Description	This command is used to force the Switch to restart.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To force the Switch to restart:

```
DES-1228/ME:4#reboot force_agree
Command: reboot force_agree

Please wait, the switch is rebooting...
```

## reset

Purpose	Used to reset the Switch to the factory default settings.
Syntax	<b>reset</b> <b>{[config   system]}</b> <b>{force_agree}</b>
Description	This command is used to restore the Switch's configuration to the default settings assigned from the factory.
Parameters	<p><i>config</i> - If the keyword 'config' is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, and the switch history log. The Switch will not save or reboot.</p> <p><i>system</i> – If the keyword 'system' is specified all of the factory default settings are restored on the Switch. The Switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base.</p> <p><i>force_agree</i> – When force_agree is specified, the reset command will be executed immediately without further confirmation.</p> <p>If no parameter is specified, the Switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The Switch will not save or reboot.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#reset config
Command: reset config

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

Success.

DES-1228/ME:4#
```

## login

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

Example usage:

To initiate the login procedure:

```
DES-1228/ME:4#login
Command: login

UserName:
```



## logout

Purpose	Used to log out a user from the Switch's console.
Syntax	<b>logout</b>
Description	This command terminates the current user's session on the Switch's console.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current user's console session:

```
DES-1228/ME:4#logout
```

## MODIFY BANNER AND PROMPT COMMANDS

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

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

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

### config command prompt

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

Example usage

To modify the command prompt to “AtYourService”:

```
DES-1228/ME:4#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:4#
```

### config greeting\_message

Purpose	Used to configure the login banner (greeting message).
Syntax	<b>config greeting_message {default}</b>
Description	Users can use this command to modify the login banner (greeting message).
Parameters	<p><i>default</i> – If the user enters <i>default</i> to the modify banner command, then the banner will be reset to the original factory banner.</p> <p>To open the Banner Editor, click <b>Enter</b> after typing the <b>config greeting_message</b> command. Type the information to be displayed on the banner by using the commands</p>

**config greeting\_message**

described on the Banner Editor:

Quit without save:      Ctrl+C  
 Save and quit:          Ctrl+W  
 Move cursor:            Left/Right/Up/Down  
 Delete line:            Ctrl+D  
 Erase all setting:      Ctrl+X  
 Reload original setting: Ctrl+L

**Restrictions**

Only Administrator-level users can issue this command. Other restrictions include:

If the "**reset/reset config**" command is executed, the modified banner will remain modified. However, the "**reset system**" command will reset the modified banner to the original factory banner.

The capacity of the banner is 6\*80. 6 Lines and 80 characters per line.

Ctrl+W will only save the modified banner in the DRAM. Users need to type the "**save**" command to save it into FLASH.

Only valid in threshold level.

**Example usage:**

To modify the banner to read "Say goodnight, Gracie":

```
DES-1228/ME:4# config greeting_message
```

```
Command: config greeting_message
```

**Greeting Messages Editor**

```
=====
```

```
DES-1228/ME Metro Ethernet Switch
Command Line Interface
```

```
Firmware: Build 1.00.B04
```

```
Copyright(C) 2009 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	<b>show greeting_message</b>
Description	This command is used to view the currently configured greeting message on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the currently configured greeting message:

```
DES-1228/ME:4#show greeting_message
```

```
Command: show greeting_message
```

```
=====
                        DES-1228/ME Metro Ethernet Switch
                        Command Line Interface

                        Firmware: Build 1.00.B04
                        Copyright(C) 2009 D-Link Corporation. All rights reserved.
=====
```

```
DES-1228/ME:4#
```

## SWITCH PORT COMMANDS

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

Command	Parameters
config ports	[<portlist>   all ] {medium_type [fiber copper]} { speed [auto   10_half   10_full   100_half   100_full   1000_full {[master   slave] }}   flow_control [enable   disable]   state [enable   disable]   learning [enable   disable]   [description <desc 32>   clear_description]   mdix [auto  normal  cross]}(1)
show ports	[<portlist>] {description   err_disabled}

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

### config ports

Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	<b>config ports [&lt;portlist&gt;   all ] {medium_type [fiber copper]} { speed [auto   10_half   10_full   100_half   100_full   1000_full {[master   slave] }}   flow_control [enable   disable]   state [enable   disable]   learning [enable   disable]   [description &lt;desc 32&gt;   clear_description]   mdix [auto  normal  cross]}(1)</b>
Description	This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.
Parameters	<p><i>all</i> – Configure all ports on the Switch.</p> <p>&lt;portlist&gt; – Specifies a port or range of ports to be configured.</p> <p><i>medium_type [fiber   copper]</i> – This applies only to the Combo ports. If configuring the Combo ports this defines the type of medium being configured.</p> <p><i>speed</i> – Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following:</p> <ul style="list-style-type: none"> <li><i>auto</i> – Enables auto-negotiation for the specified range of ports.</li> <li><i>[10   100   1000]</i> – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 but can be set to slower speeds.</li> <li><i>[half   full]</i> – Configures the specified range of ports as either full-duplex or half-duplex.</li> <li><i>[master   slave]</i> – The master setting (1000M/Full_M) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (1000M/Full_S) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for 1000M/Full_M, the other side of the connection must be set for 1000M/Full_S. Any other configuration will result in a link down status for both ports.</li> </ul> <p><i>flow_control [enable   disable]</i> – Enable or disable flow control for the specified ports.</p> <p><i>learning [enable   disable]</i> – Enables or disables the MAC address learning on the specified range of ports.</p> <p><i>state [enable   disable]</i> – Enables or disables the specified range of ports.</p> <p><i>description &lt;desc 32&gt;</i> – Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.</p> <p><i>clear_description</i> – Enter this command to clear the port description of the selected port(s).</p> <p><i>mdix</i> – Specifies the MDIX setting of the port. The MDIX setting can be auto, normal or cross.</p>

## config ports

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.

**Restrictions** Only Administrator-level users can issue this command.

Example usage:

To configure the speed of ports 1–3 to be 10 Mbps, full duplex, with learning and state enabled:

```
DES-1228/ME:4#config ports 1-3 speed 10_full state enable
```

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

```
Success.
```

```
DES-1228/ME:4#
```

## show ports

**Purpose** Used to display the current configuration of a range of ports.

**Syntax** **show ports [<portlist>] {description | err\_disabled}**

**Description** The show ports command displays the current configurations of a range of ports. No parameters will show all ports.

**Parameters**

- <portlist>* – Specifies a port or range of ports to be displayed.
- {description} – Adding this parameter to the show ports command indicates that a previously entered port description will be included in the display.
- err\_disabled* – Use this to list disabled ports including connection status and reason for being disabled.

**Restrictions** None.

Example usage:

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

```
DES-1228/ME:4#show ports
```

```
Command show ports
```

Port	State/ MDI	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
-----	-----	-----	-----	-----
1	Enabled Auto	Auto/Disabled	LinkDown	Enabled
2	Enabled Auto	Auto/Disabled	LinkDown	Enabled
3	Enabled Auto	Auto/Disabled	LinkDown	Enabled
4	Enabled Auto	Auto/Disabled	LinkDown	Enabled
5	Enabled Auto	Auto/Disabled	LinkDown	Enabled
6	Enabled Auto	Auto/Disabled	LinkDown	Enabled
7	Enabled Auto	Auto/Disabled	100M/Full/None	Enabled
8	Enabled Auto	Auto/Disabled	LinkDown	Enabled
9	Enabled Auto	Auto/Disabled	LinkDown	Enabled

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

Example usage:

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

```
DES-1228/ME:4#show ports description
```

```
Command: show ports description
```

Port	State/ MDI	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1	Enabled Auto	Auto/Disabled	LinkDown	Enabled
Desc:				
2	Enabled Auto	Auto/Disabled	LinkDown	Enabled
Desc:				
3	Enabled Auto	Auto/Disabled	LinkDown	Enabled
Desc:				
4	Enabled Auto	Auto/Disabled	LinkDown	Enabled
Desc:				
5	Enabled Auto	Auto/Disabled	LinkDown	Enabled
Desc:				
6	Enabled Auto	Auto/Disabled	LinkDown	Enabled
Desc:				

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



## PORT SECURITY COMMANDS

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

Command	Parameters
config port_security ports	[ <auth_portlist>   all ] { admin_state [enable   disable]   max_learning_addr <max_lock_no 0-64>   lock_address_mode [DeleteOnTimeout   DeleteOnReset   Permanent]}(1)
delete port_security entry	vlan_name <vlan_name 32> mac_address <macaddr> port <auth_port>
clear port_security_entry	port <auth_portlist>
show port_security	{ports <auth_portlist>}
enable port_security trap_log	
disable port_security trap_log	

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

### config port\_security ports

Purpose	Used to configure port security settings.
Syntax	<b>config port_security ports [ &lt;auth_portlist&gt;   all ] { admin_state [enable   disable]   max_learning_addr &lt;max_lock_no 0-64&gt;   lock_address_mode [DeleteOnTimeout   DeleteOnReset   Permanent]}(1)</b>
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <auth_portlist> are affected.
Parameters	<p>&lt;auth_portlist&gt; – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Configure port security for all ports on the Switch.</p> <p><i>admin_state [enable   disable]</i> – Enable or disable port security for the listed ports.</p> <p><i>max_learning_addr &lt;max_lock_no 0-64&gt;</i> – Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p><i>lock_address_mode [Permanent   DeleteOnTimeout   DeleteOnReset]</i> – Indicates the method of locking addresses. The user has three choices:</p> <ul style="list-style-type: none"> <li>▪ <i>Permanent</i> – The locked addresses will not age out.</li> <li>▪ <i>DeleteOnTimeout</i> – The locked addresses will age out after the aging timer expires (Aging Time is set using the FDB command).</li> <li>▪ <i>DeleteOnReset</i> – The locked addresses will not age out until the Switch has been reset.</li> </ul>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the port security:

```
DES-1228/ME:4#config port_security ports 1-5 admin_state enable max_learning_addr 5
lock_address_mode DeleteOnReset
Command: config port_security ports 1-5 admin_state enable max_learning_addr 5
lock_address_mode DeleteOnReset

Success.

DES-1228/ME:4#
```

## delete port\_security\_entry

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

Example usage:

To delete a port security entry:

```
DES-1228/ME:4#delete port_security_entry vlan_name default mac_address 00-01-30-10-2C-
C7 port 6
Command: delete port_security_entry vlan_name default mac_address 00-01-30-10-2C-C7
port 6

Success.

DES-1228/ME:4#
```

## clear port\_security\_entry

Purpose	Used to clear MAC address entries learned from a specified port for the port security function.
Syntax	<b>clear port_security_entry ports &lt;auth_portlist&gt;</b>
Description	This command is used to clear MAC address entries which were learned by the Switch by a specified port. This command only relates to the port security function.
Parameters	<i>&lt;auth_portlist&gt;</i> – Specifies a port or port range to clear.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear a port security entry by port:

```
DES-1228/ME:4# clear port_security_entry port 6
```

```
Command: clear port_security_entry port 6
```

```
Success.
```

```
DES-1228/ME:4#
```

## show port\_security

Purpose	Used to display the current port security configuration.
Syntax	<b>show port_security {ports &lt;auth_portlist&gt;}</b>
Description	This command is used to display port security information of the Switch's ports. The information displayed includes port security, admin state, maximum number of learning address and lock mode.
Parameters	<auth_portlist> – Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DES-1228/ME:4#show port_security ports 1-10
```

```
Command: show port_security ports 1-10
```

```
Port_security Trap/Log : Disabled
```

Port	Admin State	Max. Learning Addr.	Lock Address Mode
1	Disabled	1	DeleteOnTimeout
2	Disabled	1	DeleteOnTimeout
3	Disabled	1	DeleteOnTimeout
4	Disabled	1	DeleteOnTimeout
5	Disabled	1	DeleteOnTimeout
6	Disabled	1	DeleteOnTimeout
7	Disabled	1	DeleteOnTimeout
8	Disabled	1	DeleteOnTimeout
9	Disabled	1	DeleteOnTimeout
10	Disabled	1	DeleteOnTimeout

```
DES-1228/ME:4#
```

## enable port\_security trap\_log

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

Example usage:

To enable the port security trap log setting:

```
DES-1228/ME:4#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-1228/ME:4#
```

## disable port\_security trap\_log

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

Example usage:

To enable the port security trap log setting:

```
DES-1228/ME:4#enable port_security trap_log
Command: enable port_security trap_log

Success.

DES-1228/ME:4#
```

## NETWORK MANAGEMENT (SNMP) COMMANDS

The DES-1228/ME support the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. Users can specify which version of the SNMP users want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

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

Command	Parameters
create snmp user	<SNMP_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 >   sha <auth_password 8-20>] priv [none   des <priv_password 8-16>]   by_key auth [md5 <auth_key 32-32>   sha <auth_key 40-40>] priv [none   des <priv_key 32-32>]]}
delete snmp user	<SNMP_name 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included   excluded]
delete snmp view	<view_name 32> [all   oid]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only   read_write]
delete snmp community	<community_string 32>
show snmp community	<community_string 32>
config snmp engineID	<snmp_engineID 10-64>
show snmp engineID	
create snmp group	<groupname 32> [v1   v2   v3 [noauth_nopriv   auth_nopriv   auth_priv]][read_view <view_name 32>   write_view <view_name 32>   notify_view <view_name 32>]{1}
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	<ipaddr> {v1   v2c   v3 [noauth_nopriv   auth_nopriv   auth_priv]} <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	<ipaddr>

Command	Parameters
create trusted_host	<ipaddr>  network<network_address>
delete trusted_host	[all   ipaddr<ipaddr>  network<network_address>]
show trusted_host	
enable snmp traps	
enable snmp authenticate traps	
config stp trap	{new_root [enable disable] topo_change [enable disable]}(1)
show snmp traps	{linkchange_traps { ports <portlist>}}
disable snmp traps	
disable snmp authenticate traps	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable rmon	
disable rmon	
config snmp linkchange_traps ports	[all <portlist>] [enable disable]
enable snmp linkchange_traps	
disable snmp linkchange_traps	
config snmp coldstart_traps	[enable disable]
config snmp warmstart_traps	[enable disable]

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

## create snmp user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	<b>create snmp user &lt;SNMP_name 32&gt; &lt;groupname 32&gt; {encrypted [by_password auth [md5 &lt;auth_password 8-16&gt;   sha &lt;auth_password 8-20&gt;] priv [none   des &lt;priv_password 8-16&gt;]   by_key auth [md5 &lt;auth_key 32-32&gt;   sha &lt;auth_key 40-40&gt;] priv [none   des &lt;priv_key 32-32&gt;]]}</b>
Description	The <b>create snmp user</b> command creates a new SNMP user and adds the user to an SNMP group that is also created by this command. SNMP ensures: Message integrity – Ensures that packets have not been tampered with during transit. Authentication – Determines if an SNMP message is from a valid source. Encryption – Scrambles the contents of messages to prevent it from being viewed by an unauthorized source.
Parameters	<p>&lt;SNMP_name 32&gt; – An alphanumeric name of up to 32 characters that will identify the new SNMP user.</p> <p>&lt;groupname 32&gt; – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p><i>encrypted</i> – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose:</p> <ul style="list-style-type: none"> <li><i>by_password</i> – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the auth_password below. This method is recommended.</li> <li><i>by_key</i> – Requires the SNMP user to enter an encryption key for authentication and privacy. The key is defined by specifying the key in hex form below. This method</li> </ul>

## create snmp user

is not recommended.

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

*md5* – Specifies that the HMAC-MD5-96 authentication level will be used. md5 may be utilized by entering one of the following:

*<auth\_password 8-16>* – An alphanumeric string of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host.

*<auth\_key 32-32>* – Enter an alphanumeric string of exactly 32 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host.

*sha* – Specifies that the HMAC-SHA-96 authentication level will be used.

*<auth\_password 8-20>* – An alphanumeric string of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.

*<auth\_key 40-40>* – Enter an alphanumeric string of exactly 40 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host.

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

*des* – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using:

*<priv\_password 8-16>* – An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.

*<priv\_key 32-32>* – Enter an alphanumeric key string of exactly 32 characters, in hex form, that will be used to encrypt the contents of messages the host sends to the agent.

*none* – Adding this parameter will add no encryption.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DES-1228/ME:4#create snmp user dlink default encrypted by_password auth md5 canadian
priv none
Command: create snmp user dlink default encrypted by_password auth md5 canadian priv
none

Success.

DES-1228/ME:4#
```

## delete snmp user

Purpose	Used to remove an SNMP user from an SNMP group and also to delete the associated SNMP group.
Syntax	<b>delete snmp user &lt;SNMP_name 32&gt;</b>
Description	The <b>delete snmp user</b> command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	<i>&lt;SNMP_name 32&gt;</i> – An alphanumeric string of up to 32 characters that identifies the SNMP user that will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a previously entered SNMP user on the Switch:

```
DES-1228/ME:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DES-1228/ME:4#
```

## show snmp user

Purpose	Used to display information about each SNMP username in the SNMP group username table.
Syntax	<b>show snmp user</b>
Description	The <b>show snmp user</b> command displays information about each SNMP username in the SNMP group username table.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the SNMP users currently configured on the Switch:

```
DES-1228/ME:4#show snmp user
Command: show snmp user

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

Total Entries: 1

DES-1228/ME:4#
```

## create snmp view

Purpose	Used to assign views to community strings to limit which MIB objects and SNMP manager can access.
Syntax	<b>create snmp view &lt;view_name 32&gt; &lt;oid&gt; view_type [included   excluded]</b>
Description	The <b>create snmp view</b> command assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	<p><b>&lt;view_name 32&gt;</b> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created.</p> <p><b>&lt;oid&gt;</b> – The object ID that identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.</p> <p><b>view type</b> – Sets the view type to be:</p> <ul style="list-style-type: none"> <li><i>included</i> – Include this object in the list of objects that an SNMP manager can access.</li> <li><i>excluded</i> – Exclude this object from the list of objects that an SNMP manager can access.</li> </ul>
Restrictions	Only Administrator-level users can issue this command.



Example usage:

To create an SNMP view:

```
DES-1228/ME:4#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-1228/ME:4#
```

## delete snmp view

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

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DES-1228/ME:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-1228/ME:4#
```

## show snmp view

Purpose	Used to display an SNMP view previously created on the Switch.
Syntax	<b>show snmp view {&lt;view_name 32&gt;}</b>
Description	The <b>show snmp view</b> command displays an SNMP view previously created on the Switch.
Parameters	<i>&lt;view_name 32&gt;</i> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be displayed.
Restrictions	None.

Example usage:

To display SNMP view configuration:

DES-1228/ME:4#show snmp view

Command: show snmp view

## Vacm View Table Settings

View Name	Subtree	View Type
ReadView	1	Included
WriteView	1	Included
NotifyView	1.3.6	Included
restricted	1.3.6.1.2.1.1	Included
restricted	1.3.6.1.2.1.11	Included
restricted	1.3.6.1.6.3.10.2.1	Included
restricted	1.3.6.1.6.3.11.2.1	Included
restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included
CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Included

Total Entries: 11

DES-1228/ME:4#

**create snmp community**

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

Example usage:

To create the SNMP community string “dlink:”

```
DES-1228/ME:4#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DES-1228/ME:4#
```

## delete snmp community

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

Example usage:

To delete the SNMP community string “dlink:”

```
DES-1228/ME:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-1228/ME:4#
```

## show snmp community

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

Example usage:

To display the currently entered SNMP community strings:

```
DES-1228/ME:4#show snmp community
Command: show snmp community

SNMP Community Table

Community Name      View Name          Access Right
-----
private            CommunityView     read_write
public             CommunityView     read_only
dlink              ReadView          read_write

Total Entries: 3

DES-1228/ME:4#
```

## config snmp engineID

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

Example usage:

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

```
DES-1228/ME:4#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DES-1228/ME:4#
```

## show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the Switch.
Syntax	<b>show snmp engineID</b>
Description	The <b>show snmp engineID</b> 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-1228/ME:4#show snmp engineID
```

```
Command: show snmp engineID
```

```
SNMP Engine ID : 0035636666
```

```
DES-1228/ME:4#
```

## create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	<b>create snmp group &lt;groupname 32&gt; [v1   v2   v3 [noauth_nopriv   auth_nopriv   auth_priv]]{read_view &lt;view_name 32&gt;   write_view &lt;view_name 32&gt;   notify_view &lt;view_name 32&gt;}(1)</b>
Description	The <b>create snmp group</b> command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	<p><i>&lt;groupname 32&gt;</i> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p><i>v1</i> – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p><i>v2c</i> – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>v3</i> – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <ul style="list-style-type: none"> <li>Message integrity – Ensures that packets have not been tampered with during transit.</li> <li>Authentication – Determines if an SNMP message is from a valid source.</li> <li>Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source.</li> </ul> <p><i>noauth_nopriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_priv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manager will be encrypted.</p> <p><i>read_view</i> – Specifies that the SNMP group being created can request SNMP messages.</p> <p><i>write_view</i> – Specifies that the SNMP group being created has write privileges.</p> <p><i>notify_view</i> – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent.</p> <p><i>&lt;view_name 32&gt;</i> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP group named “sg1:”

```
DES-1228/ME:4#create snmp group sg1 v3 noauth_nopriv read_view v1 write_view v1
notify_view v1
Command: create snmp group sg1 v3 noauth_nopriv read_view v1 write_view v1 notify_view
v1

Success.

DES-1228/ME:4#
```

## delete snmp group

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

Example usage:

To delete the SNMP group named “sg1”.

```
DES-1228/ME:4#delete snmp group sg1
Command: delete snmp group sg1

Success.

DES-1228/ME:4#
```

## show snmp groups

Purpose	Used to display the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Syntax	<b>show snmp groups</b>
Description	The <b>show snmp groups</b> 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-1228/ME:4#show snmp groups
Command: show snmp groups
Vacm Access          Table Settings

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

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

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

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

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

Total Entries: 5

DES-1228/ME:4#
```

**create snmp host**

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

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-1228/ME:4#create snmp host 10.48.74.100 v3 auth_priv public
```

```
Command: create snmp host 10.48.74.100 v3 auth_priv public
```

```
Success.
```

```
DES-1228/ME:4#
```

**delete snmp host**

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



Example usage:

To delete an SNMP host entry:

```
DES-1228/ME:4#delete snmp host 10.48.74.100
```

```
Command: delete snmp host 10.48.74.100
```

```
Success.
```

```
DES-1228/ME:4#
```

## show snmp host

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

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DES-1228/ME:4#show snmp host
```

```
Command: show snmp host
```

### SNMP Host Table

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

```
Total Entries: 2
```

```
DES-1228/ME:4#
```

## create trusted\_host

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

Example usage:

To create the trusted host:

```
DES-1228/ME:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121
```

Success.

```
DES-1228/ME:4#
```

## create trusted\_host network

Purpose	Used to create the trusted host subnet.
Syntax	<b>create trusted_host network &lt;network_address&gt;</b>
Description	The create trusted host network command creates the trusted host subnet. The Switch allows users to specify up to ten IP network addresses that are allowed to manage the Switch via in-band SNMP or TELNET based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.
Parameters	<network_address> – The IP address and netmask of the trusted host to be created.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the trusted host network:

```
DES-1228/ME:4#create trusted_host network 10.48.74.121/16
Command: create trusted_host network 10.48.74.121/16
```

Success.

```
DES-1228/ME:4#
```

## show trusted\_host

Purpose	Used to display a list of trusted hosts entered on the Switch using the <b>create trusted_host</b> command above.
Syntax	<b>show trusted_host</b>
Description	This command is used to display a list of trusted hosts entered on the Switch using the <b>create trusted_host</b> command above.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To display the list of trust hosts:

```
DES-1228/ME:4#show trusted_host
```

```
Command: show trusted_host
```

```
Management Stations
```

```
IP Address/Netmask
```

```
-----
```

```
10.53.13.94
```

```
Total Entries: 1
```

```
DES-1228/ME:4#
```

## delete trusted\_host

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

Example usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DES-1228/ME:4#delete trusted_host 10.48.74.121
```

```
Command: delete trusted_host 10.48.74.121
```

```
Success.
```

```
DES-1228/ME:4#
```

## delete trusted\_host network

Purpose	Used to delete a trusted host entry made using the <b>create trusted_host network</b> command above.
Syntax	<b>delete trusted_host network &lt;network_address&gt;</b>
Description	This command is used to delete a trusted host entry made using the <b>create trusted_host network</b> command above.
Parameters	<network_address> – IP address and netmask of the trusted host network.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a trusted host network with an IP address 10.62.0.0/16:

```
DES-1228/ME:4#delete trusted_host network 10.62.0.0/16
Command: delete trusted_host network 10.62.0.0/16
```

Success.

```
DES-1228/ME:4#
```

## delete trusted\_host all

Purpose	Used to delete all trusted host entries made using the <b>create trusted_host ipaddr</b> and <b>create trusted_host network</b> commands above.
Syntax	<b>delete trusted_host all</b>
Description	This command is used to delete all trusted host entries made using the <b>create trusted_host ipaddr</b> and <b>create trusted_host network</b> commands above.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete all trusted host entries:

```
DES-1228/MEG:4# delete trusted_host all
Command: delete trusted_host all
```

Success.

## enable snmp traps

Purpose	Used to enable SNMP trap support.
Syntax	<b>enable snmp traps</b>
Description	The <b>enable snmp traps</b> command is used to enable SNMP trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SNMP trap support on the Switch:

```
DES-1228/ME:4#enable snmp traps
Command: enable snmp traps
```

Success.

```
DES-1228/ME:4#
```

## enable snmp authenticate traps

Purpose	Used to enable SNMP authentication trap support.
Syntax	<b>enable snmp authenticate traps</b>

## enable snmp authenticate traps

Description	This command is used to enable SNMP authentication trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To turn on SNMP authentication trap support:

```
DES-1228/ME:4#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DES-1228/ME:4#
```

## config stp trap

Purpose	Used to configure STP traps for SNMP.
Syntax	<b>config stp trap {new_root [enable disable]   topo_change [enable disable]}(1)</b>
Description	Used to configure STP traps for SNMP.
Parameters	<i>new_root [enable disable]</i> – The user can enable or disable the new root option. <i>topo_change [enable disable]</i> – The user can enable or diable traps when a topology change occur here.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable a new root trap:

```
DES-1228/ME:4#config stp trap new_root enable
Command: config stp trap new_root enable

Success.

DES-1228/ME:4#
```

## show snmp traps

Purpose	Used to show SNMP trap support on the Switch .
Syntax	<b>show snmp traps {linkchange_traps { ports &lt;portlist&gt;}}</b>
Description	This command is used to view the SNMP trap support status currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DES-1228/ME:4#show snmp traps
Command: show snmp traps

SNMP Traps           : Enabled
Authenticate Traps   : Enabled

DES-1228/ME:4#
```

## disable snmp traps

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

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DES-1228/ME:4#disable snmp traps
Command: disable snmp traps

Success.

DES-1228/ME:4#
```

## disable snmp authenticate traps

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

Example usage:

To disable the SNMP authentication trap support:

```
DES-1228/ME:4#disable snmp authenticate traps
Command: disable snmp authenticate traps

Success.

DES-1228/ME:4#
```

## config snmp system\_contact

Purpose	Used to enter the name of a contact person who is responsible for the Switch.
Syntax	<b>config snmp system_contact</b> {<sw_contact>}
Description	The <b>config snmp system_contact</b> 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 characters can be used.
Parameters	<sw_contact> – A maximum of 128 characters is allowed. A NULL string is accepted if there is no contact.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the Switch contact to “MIS Department II”:

```
DES-1228/ME:4#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DES-1228/ME:4#
```

## config snmp system\_location

Purpose	Used to enter a description of the location of the Switch.
Syntax	<b>config snmp system_location</b> {<sw_location>}
Description	The <b>config snmp system_location</b> command is used to enter a description of the location of the Switch. A maximum of 128 characters can be used.
Parameters	<sw_location> – A maximum of 128 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-1228/ME:4#
```

## config snmp system\_name

Purpose	Used to configure the name for the Switch.
Syntax	<b>config snmp system_name</b> {<sw_name>}
Description	The <b>config snmp system_name</b> command configures the name of the Switch.
Parameters	<sw_name> – A maximum of 128 characters is allowed. A NULL string is accepted if no name is desired.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the Switch name for “**DES-1228/ME Switch**”:

```
DES-1228/ME:4#config snmp system_name DES-1228/ME Switch
Command: config snmp system_name DES-1228/ME Switch

Success.

DES-1228/ME:4#
```

## enable rmon

Purpose	Used to enable RMON on the Switch.
Syntax	<b>enable rmon</b>
Description	This command is used, in conjunction with the <b>disable rmon</b> command below, to enable and disable remote monitoring (RMON) on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To enable RMON:

```
DES-1228/ME:4#enable rmon
Command: enable rmon

Success.

DES-1228/ME:4#
```

## disable rmon

Purpose	Used to disable RMON on the Switch.
Syntax	<b>disable rmon</b>
Description	This command is used, in conjunction with the <b>enable rmon</b> command above, to enable and disable remote monitoring (RMON) on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To disable RMON:

```
DES-1228/ME:4#disable rmon
Command: disable rmon

Success.

DES-1228/ME:4#
```



## config snmp linkchange\_traps ports

Purpose	Used to configure SNMP link changing port traps/
Syntax	<b>config snmp linkchange_traps ports [all &lt;portlist&gt;] [enable disable]</b>
Description	Used to configure SNMP link changing port traps/
Parameters	<i>all &lt;portlist&gt;</i> – The user can define either all ports or a list of port that will be configured. <i>[enable disable]</i> – The user can enable this function or disable this function for the abovementioned ports.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To enable SNMP link changing port traps:

```
DES-1228/ME:4#config snmp linkchange_traps ports all enable
Command: config snmp linkchange_traps ports all enable

Success.

DES-1228/ME:4#
```

## enable snmp linkchange\_traps

Purpose	Used to enable SNMP link changing traps on the Switch.
Syntax	<b>enable snmp linkchange_traps</b>
Description	Used to enable SNMP link changing traps on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To enable SNMP link changing traps:

```
DES-1228/ME:4#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DES-1228/ME:4#
```

## disable snmp linkchange\_traps

Purpose	Used to disable SNMP link changing traps on the Switch.
Syntax	<b>disable snmp linkchange_traps</b>
Description	Used to disable SNMP link changing traps on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To disable SNMP link changing traps:

```
DES-1228/ME:4#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DES-1228/ME:4#
```

## config snmp coldstart\_traps

Purpose	Used to configure cold start SNMP traps.
Syntax	<b>config snmp coldstart_traps [enable disable]</b>
Description	Used to configure cold start SNMP traps.
Parameters	<i>[enable disable]</i> – Choose enable or disable to enable or disable this function.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To enable config snmp coldstart\_traps:

```
DES-1228/ME:4#config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

DES-1228/ME:4#
```

## config snmp warmstart\_traps

Purpose	Used to configure warm start SNMP traps.
Syntax	<b>config snmp warmstart_traps [enable disable]</b>
Description	Used to configure warm start SNMP traps.
Parameters	<i>[enable disable]</i> – Choose enable or disable to enable or disable this function.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To enable config snmp warmstart\_traps:

```
DES-1228/ME:4#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DES-1228/ME:4#
```

## SWITCH UTILITY COMMANDS

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

Command	Parameters
download	[ firmware_fromTFTP <ipaddr> <path_filename 64> image_id <value 1-2>   cfg_fromTFTP <ipaddr> <path_filename 64> {config_id <value 1-2>   increment} ]
config firmware	image_id <int 1-2> [delete   boot_up]
show firmware information	
show config	[ current_config {[include   exclude   begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include   exclude   begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include   exclude   begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}   config_in_nvram <config_id 1-2> {[include   exclude   begin] <filter_string 80> {<filter_string 80>{<filter_string 80>}} {[include   exclude   begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include   exclude   begin] <filter_string 80>{<filter_string 80> {<filter_string 80>}}}}   information ]
upload	[ cfg_toTFTP <ipaddr> <path_filename 64> {config_id <value 1-2>} {[include   exclude   begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include   exclude   begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include   exclude   begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}   log_toTFTP <ipaddr> <path_filename 64>]
enable autoconfig	
disable autoconfig	
show autoconfig	
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
config terminal _line	[default   <value 20-80>]
show terminal line	
config configuration	config_id <value 1-2> [ delete   boot_up   active ]
config configuration trap	{save [enable disable]   upload [enable disable]   download [enable disable]}(1)

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

### download

Purpose	Used to download and install new firmware or a Switch configuration file from a TFTP server.
Syntax	<b>download [ firmware_fromTFTP &lt;ipaddr&gt; &lt;path_filename 64&gt; image_id &lt;value 1-2&gt;   cfg_fromTFTP &lt;ipaddr&gt; &lt;path_filename 64&gt; {config_id &lt;value 1-2&gt;   increment} ]</b>
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	<p><i>firmware_fromTFTP</i> – Download and install new firmware on the Switch from a TFTP server.</p> <p><i>cfg_fromTFTP</i> – Download a switch configuration file from a TFTP server.</p> <p><i>&lt;ipaddr&gt;</i> – The IP address of the TFTP server.</p> <p><i>&lt;path_filename&gt;</i> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\1228.had.</p>

## download

*image\_id <int 1-2>* – Specify the working section ID. The Switch can hold two firmware versions for the user to select from, which are specified by section ID.

*increment* – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.

### Restrictions

Only Administrator-level users can issue this command.



**Note:** The TFTP server must be on the same IP subnet as the Switch

Example usage:

To download a configuration file:

```
DES-1228/ME:4#download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt
Command: download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt

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

DES-1228/ME:4#
DES-1228/ME:4##-----
DES-1228/ME:4##                               DES-1228/ME Configuration
DES-1228/ME:4##
DES-1228/ME:4##                               Firmware: Build 1.00.B04
DES-1228/ME:4##  Copyright(C) 2009 D-Link Corporation. All rights reserved.
DES-1228/ME:4##-----
DES-1228/ME:4#
DES-1228/ME:4#
DES-1228/ME:4## BASIC
DES-1228/ME:4#
DES-1228/ME:4#config serial_port baud_rate 9600 auto_logout 10_minutes
Command: config serial_port baud_rate 9600 auto_logout 10_minutes
```

The download configuration command will initiate the loading of the various settings in the order listed in the configuration file. When the file has been successfully loaded the message “End of configuration file for DES-1228/ME” appears followed by the command prompt.

```
DES-1228/ME:4#disable authen_policy
Command: disable authen_policy

Success.

DES-1228/ME:4#
```

## config firmware

## config firmware

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

Example usage:

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

```
DES-1228/ME:4# config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DES-1228/ME:4#
```

## show firmware information

Purpose	Used to display the firmware section information.
Syntax	<b>show firmware information</b>
Description	This command is used to display the firmware section information.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the current firmware information on the Switch:

```
DES-1228/ME:4#show firmware information
Command: show firmware information

ID  Version  Size(B)  Update Time  From  User
--  -
*1  1.00.B04  1687980  0000/00/00 00:08:08  192.168.69.111(WEB)  Anonymous
 2  1.00.B03  1687456  0000/00/00 17:10:10  10.10.27.67(CONSOLE)  Anonymous

'*'      : Boot up firmware
(SSH)    : Firmware update through SSH
(WEB)    : Firmware update through WEB
(SNMP)   : Firmware update through SNMP
(TELNET) : Firmware update through TELNET
(CONSOLE): Firmware update through CONSOLE

DES-1228/ME:4#
```

**show config**

Purpose	Used to display the current or saved version of the configuration settings of the switch.
Syntax	<b>show config [ current_config {[include   exclude   begin] &lt;filter_string 80&gt; {&lt;filter_string 80&gt; {&lt;filter_string 80&gt;}} {[include   exclude   begin] &lt;filter_string 80&gt; {&lt;filter_string 80&gt; {&lt;filter_string 80&gt;}} {[include   exclude   begin] &lt;filter_string 80&gt; {&lt;filter_string 80&gt;}}}]   config_in_nvram &lt;config_id 1-2&gt; {[include   exclude   begin] &lt;filter_string 80&gt; {&lt;filter_string 80&gt;{&lt;filter_string 80&gt;}} {[include   exclude   begin] &lt;filter_string 80&gt; {&lt;filter_string 80&gt; {&lt;filter_string 80&gt;}} {[include   exclude   begin] &lt;filter_string 80&gt;{&lt;filter_string 80&gt; {&lt;filter_string 80&gt;}}}]   information ]</b>
Description	<p>Use this command to display all the configuration settings that are saved to NV RAM or display the configuration settings as they are currently configured. Use the keyboard to list settings one line at a time (Enter), one page at a time (Space) or view all (a).</p> <p>The configuration settings are listed by category in the following order:</p> <ul style="list-style-type: none"> <li>• Basic (serial port, Telnet and web management status)</li> <li>• storm control</li> <li>• IP group management</li> <li>• Syslog</li> <li>• QoS</li> <li>• port mirroring</li> <li>• traffic segmentation</li> <li>• port</li> <li>• port lock</li> <li>• 8021x</li> <li>• SNMPv3</li> <li>• management (SNMP traps RMON)</li> <li>• VLAN</li> <li>• FDB (forwarding data base)</li> <li>• MAC address table notification</li> <li>• STP</li> <li>• SSH</li> <li>• ACL</li> <li>• SNTP</li> <li>• IP route</li> <li>• LACP</li> <li>• ARP</li> <li>• IP</li> <li>• IGMP snooping</li> <li>• access authentication control (TACACS etc.)</li> <li>• Bandwidth</li> <li>• safeguard_engine</li> <li>• Banner_promp</li> <li>• SMTP</li> <li>• AAA</li> <li>• DHCP_Relay</li> </ul>
Parameters	<p><i>current_config</i> – Entering this parameter will display configurations entered without being saved to NVRAM.</p> <p><i>config_in_NVRAM</i> – Entering this parameter will display configurations entered and saved to NVRAM.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the current configuration settings:

```
DES-1228/ME:4#show config current_config
Command: show config current_config

-----
#                               DES-1228/ME Configuration
#
#                               Firmware: Build 1.00.B04
#                               Copyright(C) 2009 D-Link Corporation. All rights reserved.
#-----

# BASIC

config serial_port baud_rate 9600 auto_logout never
# ACCOUNT LIST

# ACCOUNT END

# PASSWORD ENCRYPTION
disable password encryption
config terminal_line default
enable clipaging

# STORM

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

## upload

Purpose	Used to upload the current switch settings or the switch history log to a TFTP.
Syntax	<b>upload [ <i>cfg_toTFTP</i> &lt;ipaddr&gt; &lt;path_filename 64&gt; {&lt;config_id &lt;value 1-2&gt;} {[include   exclude   begin] &lt;filter_string 80&gt; {&lt;filter_string 80&gt; {&lt;filter_string 80&gt;}} {[include   exclude   begin] &lt;filter_string 80&gt; {&lt;filter_string 80&gt; {&lt;filter_string 80&gt;}} {[include   exclude   begin] &lt;filter_string 80&gt; {&lt;filter_string 80&gt; {&lt;filter_string 80&gt;}}}]   <i>log_toTFTP</i> &lt;ipaddr&gt; &lt;path_filename 64&gt;]</b>
Description	This command is used to upload either the Switch's current settings or the Switch's history log to a TFTP server.
Parameters	<i>cfg_toTFTP</i> – Specifies that the Switch's current settings will be uploaded to the TFTP server. <i>log_toTFTP</i> – Specifies that the switch history log will be uploaded to the TFTP server. <ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. <path_filename 64> – Specifies the location of the Switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the Switch.
Restrictions	Only Administrator-level users can issue this command.



**Note:** The TFTP server must be on the same IP subnet as the Switch

Example usage:

To upload a configuration file:

```
DES-1228/ME:4#upload cfg_toTFTP 10.48.74.121 c:\cfg\log.txt
Command: upload cfg_toTFTP 10.48.74.121 c:\cfg\log.txt

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

DES-1228/ME:4#
```

## enable autoconfig

Purpose	This command is used to enable the Auto Configuration for this Switch
Syntax	<b>enable autoconfig</b>
Description	This command is used to enable the Auto Configuration for this Switch
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable auto configuration on the Switch:

```
DES-1228/ME:4#enable autoconfig
Command: enable autoconfig

Success.

DES-1228/ME:4#
```

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

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



```
DES-1228/ME Metro Ethernet Switch Command Line Interface
```

```
Firmware: Build 1.00.B04
```

```
Copyright(C) 2009 D-Link Corporation. All rights reserved.
```

```
DES-1228/ME:4#
```

```
DES-1228/ME:4#
```

```
DES-1228/ME:4#download cfg_fromTFTP 10.41.44.44 c:\cfg\setting.txt
```

```
Command: download cfg_fromTFTP 10.41.44.44 c:\cfg\setting.txt
```

```
Connecting to server..... Done.
```

```
Download configuration..... Done.
```

The very end of the autoconfig process appears like this:

```
Success.
```

```
DES-1228/ME:4#
```

```
DES-1228/ME:4## ROUTE
```

```
DES-1228/ME:4#
```

```
DES-1228/ME:4#
```

```
DES-1228/ME:4##-----
```

```
DES-1228/ME:4##      End of configuration file for DES-1228/ME
```

```
DES-1228/ME:4##-----
```

```
DES-1228/ME:4#
```

```
DES-1228/ME:4#
```



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

## disable autoconfig

Purpose	Use this to deactivate auto configuration from DHCP.
Syntax	<b>disable autoconfig</b>
Description	This instructs 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 <b>config ipif</b> command.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To stop the auto configuration function:

```
DES-1228/ME:4#disable autoconfig
Command: disable autoconfig

Success.

DES-1228/ME:4#
```

## show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	<b>show autoconfig</b>
Description	This command will list the current status of the auto configuration function.
Parameters	None.
Restrictions	None.

Example usage:

To display the autoconfig status:

```
DES-1228/ME:4#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled

DES-1228/ME:4#
```

## ping

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

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DES-1228/ME:4#ping 10.48.74.121 times 4
Command: ping 10.48.74.121

Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms

Ping statistics for 10.48.74.121
Packets: Sent =4, Received =4, Lost =0

DES-1228/ME:4#
```

## config terminal line

Purpose	Used to configure the number of rows which can be displayed at a screen.
Syntax	<b>config terminal_line [default   &lt;value 20-80&gt;]</b>
Description	Used to configure the number of rows which can be displayed on a screen. Default value is 24.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the terminal line:

```
DES-1228/ME:4# config terminal_line 30
Command: config terminal_line 30

Success.

DES-1228/ME:4#
```

## show terminal line

Purpose	Used to display the number of rows which can be displayed at a screen.
Syntax	<b>show terminal_line</b>
Description	Used to display the number of rows which can be displayed on a screen.
Parameters	None.
Restrictions	None.

Example usage:

To show the terminal line:

```
DES-1228/ME:4# show terminal_line
Command: show terminal_line

Current terminal line number : 30

DES-1228/ME:4#
```

## config configuration

Purpose	Used to configure the configuration ID.
Syntax	<b>config_id &lt;value 1-2&gt; [ delete   boot_up   active ]</b>
Description	Used to configure the configuration ID.
Parameters	<i>config_id&lt;value 1-2&gt;</i> – Specifies the configuration ID to be used.
Restrictions	None.

Example usage:

To show the config configuration:

```
DES-1228/ME:4# config configuration config_id 1 boot_up
Command: config configuration config_id 1 boot_up
```

Success.

```
DES-1228/ME:4#
```

## config configuration trap

Purpose	This command is used to configure SNMP traps for the configuration.
Syntax	<b>config configuration trap {save [enable disable]   upload [enable disable]   download [enable disable]}(1)</b>
Description	This command is used to configure SNMP traps for the configuration.
Parameters	<i>save [enable disable]</i> – The user can enable or disable the save option here. <i>upload [enable disable]</i> – The user can enable or disable the upload option here. <i>download [enable disable]</i> – The user can enable or disable the downlad option here.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure SNMP traps for the configuration:

```
DES-1228/ME:4#config configuration trap save enable upload enable download enable
Command: config configuration trap save enable upload enable download enable
```

Success.

```
DES-1228/ME:4#
```

## NETWORK MONITORING COMMANDS

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

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[cpu   ports {<portlist>}]
clear counters	ports <portlist>
clear log	
show log	index <value_list X-Y>
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> ipaddress <ipaddr> {severity [informational   warning   all]   facility [local0   local1   local2   local3   local4   local5   local6   local7]   udp_port <udp_port_number>   state [enable   disable]}
config syslog host	[all   <index 1-4>] {severity [informational   warning   all]   facility [local0   local1   local2   local3   local4   local5   local6   local7]   udp_port <udp_port_number>   ipaddress <ipaddr>   state [enable   disable]}
delete syslog host	[<index 1-4>   all]
show syslog host	<index 1-4>
config log_save_timing	[time_interval <min 1-65535>   on_demand   log_trigger]
show log_save_timing	

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

### show packet ports

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

Example usage:

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

```
DES-1228/ME:4#show packet ports 2
Command: show packet ports 2

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

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

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

## show error ports

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

Example usage:

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

```
DES-1228/ME:4#show error ports 3
Command: show error ports 3

Port Number : 3

RX Frames
-----
CRC Error      0
Undersize      0
Oversize       0
Fragment       0
Jabber         0
Drop Pkts      0

Excessive Deferral 0
CRC Error           0
Late Collision      0
Excessive Collision 0
Single Collision    0
Collision           0

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

**show utilization**

Purpose	Used to display real-time port and CPU utilization statistics.
Syntax	<b>show utilization [cpu   ports {&lt;portlist&gt;}]</b>
Description	This command will display the real-time port and CPU utilization statistics for the Switch.
Parameters	<i>cpu</i> – Entering this parameter will display the current cpu utilization of the Switch. <i>ports</i> – Entering this parameter will display the current port utilization of the Switch. <ul style="list-style-type: none"> <li>▪ <i>&lt;portlist&gt;</i> – Specifies a port or range of ports to be displayed.</li> </ul>
Restrictions	None.

Example usage:

To display the port utilization statistics:

```
DES-1228/ME:4#show utilization ports
```

```
Command: show utilization ports
```

Port	TX/sec	RX/sec	Util	Port	TX/sec	RX/sec	Util
1	0	0	0	22	0	0	0
2	0	0	0	23	0	0	0
3	0	0	0	24	0	0	0
4	0	0	0	25	0	0	0
5	0	0	0	26	0	0	0
6	0	0	0	27	0	0	0
7	0	37	1	28	0	0	0
8	0	0	0				
9	0	0	0				
10	0	0	0				
11	36	0	1				
12	0	0	0				
13	0	0	0				
14	0	0	0				
15	0	0	0				
16	0	0	0				
17	0	0	0				
18	0	0	0				
19	0	0	0				
20	0	0	0				
21	0	0	0				

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

To display the current CPU utilization:

```
DES-1228/ME:4#show utilization cpu
```

```
Command: show utilization cpu
```

```
CPU utilization :
```

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

```
DES-1228/ME:4#
```

## clear counters

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

Example usage:

To clear the counters:

```
DES-1228/ME:4#clear counters ports 2-9
```

```
Command: clear counters ports 2-9
```

```
Success.
```

```
DES-1228/ME:4#
```

## clear log

Purpose	Used to clear the Switch's history log.
Syntax	<b>clear log</b>
Description	This command will clear the Switch's history log.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear the log information:

```
DES-1228/ME:4#clear log
```

```
Command: clear log
```

```
Success.
```

```
DES-1228/ME:4#
```

## show log

Purpose	Used to display the switch history log.
Syntax	<b>show log {index &lt;value_list X-Y&gt;}</b>
Description	This command will display the contents of the Switch's history log.
Parameters	<i>index &lt;value_list X-Y&gt;</i> – This command will display the history log, beginning and ending at the value specified by the user in the <value_list X-Y> field. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.



Example usage:

To display the switch history log:

```
DES-1228/ME:4#show log index 1-5
Command: show log index 1-5

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

DES-1228/ME:4#
```

## enable syslog

Purpose	Used to enable the system log to be sent to a remote host.
Syntax	<b>enable syslog</b>
Description	The <b>enable syslog</b> command enables the system log to be sent to a remote host.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To the syslog function on the Switch:

```
DES-1228/ME:4#enable syslog
Command: enable syslog

Success.

DES-1228/ME:4#
```

## disable syslog

Purpose	Used to enable the system log to be sent to a remote host.
Syntax	<b>disable syslog</b>
Description	The <b>disable syslog</b> command enables the system log to be sent to a remote host.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DES-1228/ME:4#disable syslog
Command: disable syslog

Success.

DES-1228/ME:4#
```

## show syslog

Purpose	Used to display the syslog protocol status as enabled or disabled.
Syntax	<b>show syslog</b>
Description	The <b>show syslog</b> command displays the syslog status as enabled or disabled.
Parameters	None.
Restrictions	None.

Example usage:

To display the current status of the syslog function:

```
DES-1228/ME:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-1228/ME:4#
```

## create syslog host

Purpose	Used to create a new syslog host.				
Syntax	<b>create syslog host</b> <index 1-4> <b>ipaddress</b> <ipaddr> {severity [ <b>informational</b>   <b>warning</b>   <b>all</b> ]   facility [ <b>local0</b>   <b>local1</b>   <b>local2</b>   <b>local3</b>   <b>local4</b>   <b>local5</b>   <b>local6</b>   <b>local7</b> ]   <b>udp_port</b> <udp_port_number>   state [ <b>enable</b>   <b>disable</b> ]}				
Description	The <b>create syslog host</b> command is used to create a new syslog host.				
Parameters	<p>&lt;index 1-4&gt; – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p><i>ipaddress</i> &lt;ipaddr&gt; – Specifies the IP address of the remote host where syslog messages will be sent.</p> <p><i>severity</i> – Severity level indicator. These are described in the following:  <b>Bold font</b> indicates that the corresponding severity level is currently supported on the Switch.</p> <table border="1"> <thead> <tr> <th>Numerical Code</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Numerical Code	Severity		
Numerical Code	Severity				

**create syslog host**

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

<b>Numerical Code</b>	<b>Facility</b>
-----------------------	-----------------

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
<b>16</b>	<b>local use 0 (local0)</b>
<b>17</b>	<b>local use 1 (local1)</b>
<b>18</b>	<b>local use 2 (local2)</b>
<b>19</b>	<b>local use 3 (local3)</b>
<b>20</b>	<b>local use 4 (local4)</b>
<b>21</b>	<b>local use 5 (local5)</b>
<b>22</b>	<b>local use 6 (local6)</b>
<b>23</b>	<b>local use 7 (local7)</b>

*local0* – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above.

*local1* – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above.

*local2* – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above.

*local3* – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.

*local4* – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.

*local5* – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.

*local6* – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.

*local7* – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.

*udp\_port* <udp\_port\_number> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.

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

## create syslog host

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

Example usage:

To create syslog host:

```
DES-1228/ME:4#create syslog host 1 severity all facility local0
```

```
Command: create syslog host 1 severity all facility local0
```

```
Success.
```

```
DES-1228/ME:4#
```

## config syslog host

**Purpose** Used to configure the syslog protocol to send system log data to a remote host.

**Syntax** `config syslog host [all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}`

**Description** The **config syslog host** command is used to configure the syslog protocol to send system log information to a remote host.

**Parameters**

*<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.

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

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

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

Numerical Code	Severity
----------------	----------

0	Emergency: system is unusable
---	-------------------------------

1	Alert: action must be taken immediately
---	---

2	Critical: critical conditions
---	-------------------------------

3	Error: error conditions
---	-------------------------

<b>4</b>	<b>Warning: warning conditions</b>
----------	------------------------------------

5	Notice: normal but significant condition
---	--

<b>6</b>	<b>Informational: informational messages</b>
----------	--

7	Debug: debug-level messages
---	-----------------------------

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

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

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

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

Parameters	<b>Numerical Code</b>	<b>Facility</b>
	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
	<b>16</b>	<b>local use 0 (local0)</b>
	<b>17</b>	<b>local use 1 (local1)</b>
	<b>18</b>	<b>local use 2 (local2)</b>
	<b>19</b>	<b>local use 3 (local3)</b>
	<b>20</b>	<b>local use 4 (local4)</b>
	<b>21</b>	<b>local use 5 (local5)</b>
	<b>22</b>	<b>local use 6 (local6)</b>
	<b>23</b>	<b>local use 7 (local7)</b>
Parameters	<p><i>local0</i> – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above.</p> <p><i>local1</i> – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above.</p> <p><i>local2</i> – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above.</p> <p><i>local3</i> – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.</p> <p><i>local4</i> – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.</p> <p><i>local5</i> – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.</p> <p><i>local6</i> – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.</p> <p><i>local7</i> – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.</p> <p><i>udp_port</i> &lt;<i>udp_port_number</i>&gt; – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.</p> <p><i>state</i> [<i>enable</i>   <i>disable</i>] – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.</p>	
Restrictions	Only Administrator-level users can issue this command.	

Example usage:

To configure a Syslog host:

```
DES-1228/ME:4#config syslog host 1 severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DES-1228/ME:4#
```

Example usage:

To configure a Syslog host for all hosts:

```
DES-1228/ME:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DES-1228/ME:4#
```

## delete syslog host

Purpose	Used to remove a syslog host that has been previously configured, from the Switch.
Syntax	<b>delete syslog host</b> [<index 1-4>   all]
Description	The <b>delete syslog host</b> command is used to remove a syslog host that has been previously configured from the Switch.
Parameters	<index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. all – Specifies that the command will be applied to all hosts.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DES-1228/ME:4#delete syslog host 4
Command: delete syslog host 4

Success.

DES-1228/ME:4#
```

## show syslog host

Purpose	Used to display the syslog hosts currently configured on the Switch.
Syntax	<b>show syslog host</b> {<index 1-4>}
Description	The <b>show syslog host</b> command is used to display the syslog hosts that are currently configured on the Switch.
Parameters	<index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.
Restrictions	None.

Example usage:

To show Syslog host information:

```
DES-1228/ME:4#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host Id   Host IP Address   Severity           Facility   UDP port   Status
-----
1         10.1.1.2         All                Local0    514        Disabled
2         10.40.2.3        All                Local0    514        Disabled
3         10.21.13.1       All                Local0    514        Disabled

Total Entries : 3

DES-1228/ME:4#
```

## config log\_save\_timing

Purpose	Used to configure the method of saving log files to the switch's flash memory.
Syntax	<b>config log_save_timing [time_interval &lt;min 1-65535&gt;   on_demand   log_trigger]</b>
Description	The <b>config log_save_timing</b> command allows the user to configure the time method used in saving log files to the switch's flash memory.
Parameters	<p><i>time_interval</i> &lt;min 1-65535&gt; – Use this parameter to configure the time interval that will be implemented for saving log files. The log files will be save every x number of minutes that are configured here.</p> <p><i>on_demand</i> – Users who choose this method will only save log files when they manually tell the Switch to do so, using the <b>save</b> or <b>save log</b> command.</p> <p><i>log_trigger</i> – Users who choose this method will have log files saved to the Switch every time a log event occurs on the Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the time interval as every 30 minutes for saving log files:

```
DES-1228/ME:4#config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

DES-1228/ME:4#
```

## show log\_save\_timing

Purpose	Used to display the method configured for saving log files to the switch's flash memory.
Syntax	<b>show log_save_timing</b>
Description	The <b>show log_save_timing</b> command allows the user to view the time method configured for saving log files to the switch's flash memory.
Parameters	None.
Restrictions	None.

Example usage:

To display the time interval for saving log files:

```
DES-1228/ME:4#show log_save_timing
Command: show log_save_timing

Saving log method: time_interval
                  Interval : 30

DES-1228/ME:4#
```



## MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS

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

- A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **config stp mst\_config\_id** command as *name <string>*).
- A configuration revision number (named here as a *revision\_level*) and;
- A 4094 element table (defined here as a *vid\_range*) which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

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

1. The Switch must be set to the MSTP setting (*config stp version*)
2. The correct spanning tree priority for the MSTP instance must be entered (*config stp priority*).
3. VLANs that will be shared must be added to the MSTP Instance ID (*config stp instance\_id*).

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

Command	Parameters
enable stp	
disable stp	
config stp version	[mstp   rstp   stp]
config stp	{maxage <value 6-40> maxhops <value 6-40>  hellotime <value 1-2>  forwarddelay <value 4-30> txholdcount <value 1-10> fbpdu [enable disable]    lbd [enable disable]  lbd_recover_timer [<value 0>   <value 60-1000000>]}(1)
config stp ports	<portlist> {externalCost [auto   <value 1-200000000>]   hellotime <value 1-2>   migrate [yes no]  edge [true false auto]   restricted_role [true false]  restricted_tcn [true false]   p2p [true false auto]  state [enable disable]   lbd [enable disable]   fbpdu [enable disable]}(1)
create stp instance_id	<value 1-8>
config stp instance_id	<value 1-8> [add_vlan remove_vlan] <vidlist>
delete stp instance_id	<value 1-8>
config stp priority	<value 0-61440> instance_id <value 0-8>
config stp mst_config_id	{revision_level <int 0-65535>   name <string>}(1)
config stp mst_ports	<portlist> instance_id <value 0-8> {internalCost [auto   <value 1-200000000>]} priority <value 0-240>}(1)
show stp	
show stp ports	{<portlist>} {instance <value 0-8>}
show stp instance	{<value 0-8>}

Command	Parameters
show stp mst_config id	

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

## enable stp

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

Example usage:

To enable STP, globally, on the Switch:

```
DES-1228/ME:4#enable stp
Command: enable stp

Success.

DES-1228/ME:4#
```

## disable stp

Purpose	Used to globally disable STP on the Switch.
Syntax	<b>disable stp</b>
Description	This command allows the Spanning Tree Protocol to be globally disabled on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DES-1228/ME:4#disable stp
Command: disable stp

Success.

DES-1228/ME:4#
```

## config stp version

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

## config stp version

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-1228/ME:4#config stp version mstp
```

```
Command: config stp version mstp
```

```
Success.
```

```
DES-1228/ME:4#
```

## config stp

Purpose Used to setup STP, RSTP and MSTP on the Switch.

Syntax **config stp {maxage <value 6-40>|maxhops <value 6-40> |hellotime <value 1-2>|forwarddelay <value 4-30> txholdcount <value 1-10>|fbpdu [enable|disable] | |lbd [enable|disable] |lbd\_recover\_timer [<value 0> | <value 60-1000000>]}(1)**

Description This command is used to setup the Spanning Tree Protocol (STP) for the entire Switch. All commands here will be implemented for the STP version that is currently set on the Switch.

Parameters

*maxage <value 6-40>* – This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20.

*maxhops <value 6-40>* – The number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 6 to 40. The default is 20.

*hellotime <value 1-2>* – The user may set the time interval between transmission of configuration messages by the root device, thus stating that the Switch is still functioning. A time between 1 and 2 seconds may be chosen, with a default setting of 2 seconds.



**NOTE:** In MSTP, the spanning tree is configured by port and therefore, the *hellotime* must be set using the *configure stp ports* command for switches utilizing the Multiple Spanning Tree Protocol.

*forwarddelay <value 4-30>* – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds.

*txholdcount <1-10>* – The maximum number of BPDU Hello packets transmitted per interval. Default value = 6.

*fbpdu [enable | disable]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *enable*.

*lbd [enable | disable]* – Enabling this feature temporarily block STP on the Switch when a BPDU packet has been looped back to the switch. When the Switch detects its own BPDU packet coming back, it signifies a loop on the network. STP will automatically be blocked and an alert will be sent to the administrator. The LBD STP port will restart (change to discarding state) when the **LBD Recover Time** times out. The default is enabled.

## config stp

*lbd\_recover\_timer* [0 | <value 60-1000000>] – This field will set the time the STP port will wait before recovering the STP state set. 0 will denote that the LBD will never time out or restart until the administrator personally changes it. The user may also set a time between 60 and 1000000 seconds. The default is 60 seconds.

**Restrictions** Only Administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DES-1228/ME:4#config stp maxage 18 maxhops 15
```

```
Command: config stp maxage 18 maxhops 15
```

```
Success.
```

```
DES-1228/ME:4#
```

## config stp ports

Purpose	Used to setup STP on the port level.
Syntax	<b>config stp ports</b> <portlist> {externalCost [auto   <value 1-200000000>]   hellotime <value 1-2>   migrate [yes no]   edge [true false auto]   restricted_role [true false]   restricted_tcn [true false]   p2p [true false auto]   state [enable disable]   lbd [enable disable]   fbpdudisable}(1)
Description	This command is used to create and configure STP for a group of ports.
Parameters	<p>&lt;portlist&gt; – Specifies a range of ports to be configured.</p> <p><i>externalCost</i> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is <i>auto</i>.</p> <p><i>auto</i> – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.</p> <p>&lt;value 1-200000000&gt; – Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.</p> <p><i>hellotime</i> &lt;value 1-2&gt; – 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.</p> <p><i>migrate</i> [yes   no] – Setting this parameter as “yes” will set the ports to send out BDPUs packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1D STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1D network connects</p>

**config stp ports**

to an 802.1w or 802.1s enabled network. Migration should be set as *yes* on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment.

*edge [true | false | auto]* – *true* designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status.

*p2p [true | false | auto]* – *true* indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A *p2p* value of *false* indicates that the port cannot have *p2p* status. *Auto* allows the port to have *p2p* status whenever possible and operate as if the *p2p* status were *true*. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the *p2p* status changes to operate as if the *p2p* value were *false*. The default setting for this parameter is *auto*.

*state [enable | disable]* – Allows STP to be enabled or disabled for the ports specified in the port list. The default is *enable*.

*restricted\_role* – To decide if this is to be selected as the Root Port. The default value is *false*.

*restricted\_tcn* – To decide if this port is to propagate topology change. The default value is *false*.

*lbd [enable | disable]* – Used to enable or disable the loop-back detection function on the switch for the ports configured above in the *config stp* command.

*fbpdu [enable | disable]* – When enabled, this allows the forwarding of STP BPDU packets from other network devices when STP is disabled in the specified ports. If users want to enable Forwarding BPDU on a per port basis, the following settings must first be in effect: 1. STP must be globally disabled and 2. Forwarding BPDU must be globally enabled. To globally disable STP, use the **disable stp** command, to globally enable *fbpdu*, use the **config stp** command. The default is *enable*.

**Restrictions**

Only Administrator-level users can issue this command.

Example usage:

To configure STP with path cost auto, hellotime set to 2 seconds, migration enable, and state enable for ports 1-2 of module 1.

```
DES-1228/ME:4#config stp ports 1-2 externalCost auto hellotime 2 migrate yes state
enable
Command: config stp ports 1-2 externalCost auto hellotime 2 migrate yes state en
able
DES-1228/ME:4#
```

## create stp instance\_id

Purpose	Used to create a STP instance ID for MSTP.
Syntax	<b>create stp instance_id &lt;value 1-8&gt;</b>
Description	This command allows the user to create a STP instance ID for the Multiple Spanning Tree Protocol. There are 9 STP instances on the Switch (one internal CIST, unchangeable) and the user may create up to 8 instance IDs for the Switch.
Parameters	<value 1-8> – Enter a value between 1 and 8 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a spanning tree instance 2:

```
DES-1228/ME:4#create stp instance_id 2
Command: create stp instance_id 2

Success.

DES-1228/ME:4#
```

## config stp instance\_id

Purpose	Used to add or delete an STP instance ID.
Syntax	<b>config stp instance_id &lt;value 1-8&gt; [add_vlan   remove_vlan] &lt;vidlist&gt;</b>
Description	This command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an <i>instance_id</i> . 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 9 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time. <div data-bbox="445 1648 555 1760" data-label="Image"> </div> <p><b>NOTE:</b> Switches in the same spanning tree region having the same STP <i>instance_id</i> must be mapped identically, and have the same configuration <i>revision_level</i> number and the same <i>name</i>.</p>
Parameters	<p>&lt;value 1-8&gt; – Enter a number between 1 and 8 to define the <i>instance_id</i>. The Switch supports 9 STP instances with one unchangeable default instance ID set as 0.</p> <p><i>add_vlan</i> – Along with the <i>vid_range &lt;vidlist&gt;</i> parameter, this command will add VIDs to the previously configured STP <i>instance_id</i>.</p> <p><i>remove_vlan</i> – Along with the <i>vid_range &lt;vidlist&gt;</i> parameter, this command will remove VIDs to the previously configured STP <i>instance_id</i>.</p> <p>&lt;vidlist&gt; – Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.</p>

## config stp instance\_id

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

Example usage:

To configure instance ID 2 to add VID 10:

```
DES-1228/ME:4#config stp instance_id 2 add_vlan 10
```

```
Command : config stp instance_id 2 add_vlan 10
```

```
Success.
```

```
DES-1228/ME:4#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DES-1228/ME:4#config stp instance_id 2 remove_vlan 10
```

```
Command : config stp instance_id 2 remove_vlan 10
```

```
Success.
```

```
DES-1228/ME:4#
```

## delete stp instance\_id

Purpose	Used to delete a STP instance ID from the Switch.
Syntax	<b>delete stp instance_id &lt;value 1-8&gt;</b>
Description	This command allows the user to delete a previously configured STP instance ID from the Switch.
Parameters	<value 1-8> – Enter a value between 1 and 8 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete STP instance ID 2 from the Switch.

```
DES-1228/ME:4#delete stp instance_id 2
```

```
Command: delete stp instance_id 2
```

```
Success.
```

```
DES-1228/ME:4#
```

## config stp priority

Purpose	Used to update the STP instance configuration
Syntax	<b>config stp priority &lt;value 0-61440&gt; instance_id &lt;value 0-8&gt;</b>
Description	This command is used to update the STP instance configuration settings on the Switch. The MSTP will utilize the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions will instruct the Switch to give precedence to the selected <i>instance_id</i> for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	<i>priority</i> <value 0-61440> – Select a value between 0 and 61440 to specify the priority for a specified instance ID for forwarding packets. The lower the value, the higher the priority.

## config stp priority

This entry must be divisible by 4096.

*instance\_id* <value 0-8> – Enter the value corresponding to the previously configured instance ID of which the user wishes to set the priority value. An instance id of 0 denotes the default *instance\_id* (CIST) internally set on the Switch.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To set the priority value for *instance\_id* 2 as 4096.

```
DES-1228/ME:4#config stp priority 4096 instance_id 2
```

```
Command : config stp priority 4096 instance_id 2
```

Success.

```
DES-1228/ME:4#
```

## config stp mst\_config\_id

Purpose Used to update the MSTP configuration identification.

Syntax **config stp mst\_config\_id {revision\_level <int 0-65535> | name <string>}(1)**

Description This command will uniquely identify the MSTP configuration currently configured on the Switch. Information entered here will be attached to BPDU packets as an identifier for the MSTP region to which it belongs. Switches having the same *revision\_level* and *name* will be considered as part of the same MSTP region.

Parameters *revision\_level* <int 0-65535> – Enter a number between 0 and 65535 to identify the MSTP region. This value, along with the name will identify the MSTP region configured on the Switch. The default setting is 0.

*name* <string 32> – Enter an alphanumeric string of up to 32 characters to uniquely identify the MSTP region on the Switch. This *name*, along with the *revision\_level* value will identify the MSTP region configured on the Switch. If no *name* is entered, the default name will be the MAC address of the device.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the MSTP region of the Switch with *revision\_level* 10 and the *name* “Trinity”:

```
DES-1228/ME:4#config stp mst_config_id revision_level 10 name Trinity
```

```
Command : config stp mst_config_id revision_level 10 name Trinity
```

Success.

```
DES-1228/ME:4#
```

## config stp mst\_ports

Purpose Used to update the port configuration for a MSTP instance.

Syntax **config stp mst\_ports <portlist> instance\_id <value 0-8> {internalCost [auto | <value 1-200000000>]| priority <value 0-240>}(1)**

Description This command will update the port configuration for a STP *instance\_id*. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In



**config stp mst\_ports**

	instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	<p><i>&lt;portlist&gt;</i> – Specifies a port or range of ports to be configured.</p> <p><i>instance_id &lt;value 0-8&gt;</i> – Enter a numerical value between 0 and 8 to identify the <i>instance_id</i> previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree).</p> <p><i>internalCost</i> – This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is <i>auto</i>. There are two options:</p> <ul style="list-style-type: none"> <li><i>auto</i> – Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.</li> <li><i>value 1-200000000</i> – Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower <i>internalCost</i> represents a quicker transmission.</li> </ul> <p><i>priority &lt;value 0-240&gt;</i> – Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16
Command : config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16
```

Success.

```
DES-1228/ME:4#
```

**show stp**

Purpose	Used to display the Switch's current STP configuration.
Syntax	<b>show stp</b>
Description	This command displays the Switch's current STP configuration.
Parameters	None
Restrictions	None.

Example usage:

To display the status of STP on the Switch:

**Status 1: STP enabled with STP compatible version**

```
DES-1228/ME:4#show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status      : Enabled
STP Version     : STP compatible
Max Age        : 20
Hello Time     : 2
Forward Delay  : 15
```

```

Max Hops           : 20
TX Hold Count     : 6
Forwarding BPDU   : Enabled
Loopback Detection : Enabled
LBD Recover Time  : 60

```

```
DES-1228/ME:4#
```

#### Status 2 : STP enabled for RSTP

```
DES-1228/ME:4#show stp
```

```
Command: show stp
```

#### STP Bridge Global Settings

```

-----
STP Status           : Enabled
STP Version          : RSTP
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15
Max Hops             : 20
TX Hold Count        : 6
Forwarding BPDU     : Enabled
Loopback Detection   : Enabled
LBD Recover Time     : 60

```

```
DES-1228/ME:4#
```

#### Status 3 : STP enabled for MSTP

```
DES-1228/ME:4#show stp
```

```
Command: show stp
```

#### STP Bridge Global Settings

```

-----
STP Status           : Enabled
STP Version          : MSTP
Max Age              : 20
Forward Delay        : 15
Max Hops             : 20
TX Hold Count        : 6
Forwarding BPDU     : Enabled
Loopback Detection   : Enabled
LBD Recover Time     : 60

```

```
DES-1228/ME:4#
```

## show stp ports

Purpose	Used to display the Switch's current STP ports configuration.
Syntax	<b>show stp ports {&lt;portlist&gt;} {instance &lt;value 0-8&gt;}</b>
Description	This command displays the STP ports settings for a specified port or group of ports (one port at a time).
Parameters	<portlist> – Specifies a port or range of ports to be viewed. Information for a single port is displayed. If no ports are specified the STP information for port 1 will be displayed. Users

**show stp ports**

may use the Space bar, p and n keys to view information for the remaining ports.

Restrictions None.

Example usage:

To show STP ports information for port 1 (STP enabled on Switch):

```
DES-1228/ME:4#show stp ports
Command: show stp ports

MSTP Port Information
-----
Port Index      : 1      , Hello Time: 2 /2 , Port STP Enabled  , LBD : No
Restricted role  : False,  Restricted TCN : False
External PathCost : Auto/200000  , Edge Port : False/No , P2P : Auto /Yes
Port Forward BPDU : Enabled
MSTI   Designated Bridge   Internal PathCost   Prio   Status       Role
-----
0      N/A                  200000             128    Disabled     Disabled

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

**show stp instance\_id**

Purpose	Used to display the Switch's STP instance configuration
Syntax	<b>show stp instance_id &lt;value 0-8&gt;</b>
Description	This command displays the Switch's current STP Instance Settings and the STP Instance Operational Status.
Parameters	<value 0-8> – Enter a value defining the previously configured <i>instance_id</i> on the Switch. An entry of 0 will display the STP configuration for the CIST internally set on the Switch.
Restrictions	None

Example usage:

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

```

DES-1228/ME:4#show stp instance 0
Command: show stp instance 0

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

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

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

```

## show stp mst\_config\_id

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

Example usage:

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

```

DES-1228/ME:4#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
-----

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

DES-1228/ME:4#

```

## FORWARDING DATABASE COMMANDS

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

Command	Parameters
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add   delete] <portlist>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32>   port <port>   all]
show multicast_fdb	{vlan <vlan_name 32>   mac_address <macaddr>}
show fdb	{port <port>   vlan <vlan_name 32>   vlanid <vidlist>  mac_address <macaddr>   static   aging_time}
config multicast port_filtering_mode	[<portlist>   all] [forward_unregistered_groups   filter_unregistered_groups]
show multicast port_filtering_mode	
enable flood_fdb	
config flood_fdb	{log [enable disable]  trap [enable disable]}(1)
show flood_fdb	
disable flood_fdb	
clear flood_fdb	
create auto_fdb	<ipaddr>
show auto_fdb	{<ipaddr>}
delete auto_fdb	<ipaddr>

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

### create fdb

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

Example usage:

To create a unicast MAC FDB entry:

```
DES-1228/ME:4#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DES-1228/ME:4#
```

## create multicast\_fdb

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

Example usage:

To create multicast MAC forwarding:

```
DES-1228/ME:4#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DES-1228/ME:4#
```

## config multicast\_fdb

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

Example usage:

To add multicast MAC forwarding:

```
DES-1228/ME:4#config multicast_fdb default 01-00-00-00-00-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1-5

Success.

DES-1228/ME:4#
```

## config fdb aging\_time

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

Example usage:

To set the fdb aging time:

```
DES-1228/ME:4#config fdb aging_time 300
```

```
Command: config fdb aging_time 300
```

```
Success.
```

```
DES-1228/ME:4#
```

## delete fdb

Purpose	Used to delete an entry to the Switch's forwarding database.
Syntax	<b>delete fdb &lt;vlan_name 32&gt; &lt;macaddr&gt;</b>
Description	This command is used to delete a previous entry to the Switch's MAC address forwarding database.
Parameters	<vlan_name 32> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DES-1228/ME:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DES-1228/ME:4#
```

To delete a multicast FDB entry:

```
DES-1228/ME:4#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DES-1228/ME:4#
```

## clear fdb

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

Example usage:

To clear all FDB dynamic entries:

```
DES-1228/ME:4#clear fdb all
Command: clear fdb all

Success.

DES-1228/ME:4#
```



## show multicast\_fdb

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

Example usage:

To display multicast MAC address table:

```
DES-1228/ME:4#show multicast_fdb vlan default
Command: show multicast_fdb vlan default
```

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

```
Total Entries : 1
```

```
DES-1228/ME:4#
```

## show fdb

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

Example usage:

To display unicast MAC address table:

```
DES-1228/ME:4#show fdb
```

```
Command: show fdb
```

```
Unicast MAC Address Ageing Time = 300
```

VID	VLAN Name	MAC Address	Port	Type
1	default	00-00-51-43-70-00	10	Dynamic

1	default	00-00-5E-00-01-01	10	Dynamic
1	default	00-00-74-60-72-2D	10	Dynamic
1	default	00-00-81-05-00-80	10	Dynamic
1	default	00-00-81-05-02-00	10	Dynamic
1	default	00-00-81-48-70-01	10	Dynamic
1	default	00-00-E2-4F-57-03	10	Dynamic
1	default	00-00-E2-61-53-18	10	Dynamic
1	default	00-00-E2-6B-BC-F6	10	Dynamic
1	default	00-00-E2-7F-6B-53	10	Dynamic
1	default	00-00-E2-82-7D-90	10	Dynamic
1	default	00-00-F8-7C-1C-29	10	Dynamic
1	default	00-01-02-03-04-00	CPU	Self
1	default	00-01-02-03-04-05	10	Dynamic
1	default	00-01-30-10-2C-C7	10	Dynamic
1	default	00-01-30-FA-5F-00	10	Dynamic
1	default	00-02-3F-63-DD-68	10	Dynamic

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

## config multicast port\_filtering\_mode

Purpose	Used to configure the multicast packet filtering mode on a port per port basis.
Syntax	<b>config multicast port_filtering_mode</b> [<portlist>   all] [forward_unregistered_groups   filter_unregistered_groups]
Description	This command will configure the multicast packet filtering mode for specified ports on the Switch.
Parameters	<i>[&lt;portlist&gt;   all]</i> – Enter a port or list of ports for which to configure the multicast port filtering mode. Entering the <i>all</i> parameter will denote all ports on the switch. <i>[forward_unregistered_groups   filter_unregistered_groups]</i> – The user may set the filtering mode to any of these three options.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#config multicast port_filtering_mode 1-4 forward_unregistered_groups
Command: config multicast port_filtering_mode 1-4 forward_unregistered_groups
```

Success.

```
DES-1228/ME:4#
```

## show multicast port\_filtering\_mode

Purpose	Used to show the multicast packet filtering mode on a port per port basis.
Syntax	<b>show multicast port_filtering_mode</b>
Description	This command will display the current multicast packet filtering mode for specified ports on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the multicast port filtering mode for all ports:

```
DES-1228/ME:4#show multicast port_filtering_mode
Command: show multicast port_filtering_mode

Multicast Filter Mode For Unregistered Group:
      Forwarding List: 1-28
      Filtering List:

DES-1228/ME:4#
```

## enable flood\_fdb

Purpose	Used to enable flooding MAC function.
Syntax	<b>enable flood_fdb</b>
Description	The enable flood_fdb command is used to enable flooding MAC function. The default is disabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable flood fdb:

```
DES-1228/ME:4#enable flood_fdb
Command: enable flood_fdb

Success.

DES-1228/ME:4#
```

## config flood\_fdb

Purpose	Used to configure the flooding MAC function.
Syntax	<b>config flood_fdb {log [enable disable]} trap [enable disable]}(1)</b>
Description	The config flood_fdb command is used to enable/disable log/trap state.
Parameters	<i>log [enable disable]</i> – The user can enable or disable logging here. <i>trap [enable disable]</i> – The user can enable or disable traps here.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable log state:

```
DES-1228/ME:4#config flood_fdb log enable trap enable
Command: config flood_fdb log enable trap enable

Success.

DES-1228/ME:4#
```

**show flood\_fdb**

Purpose	Used to show the flooding Flood Database.
Syntax	<b>show flood_fdb</b>
Description	The show flood_fdb command is used to display flooding MAC function state and flooding database.
Parameters	None.
Restrictions	None.

Example usage:

To display the global information of the flooding MAC function and the flooding FDB:

```
DES-1228/ME:4#show flood_fdb
Command: show flood_fdb

Flooding FDB State : Enabled
Log State           : Enabled
Trap State          : Enabled

Value  VLAN ID  MAC Address           Time Stamp
-----  -----  -
1722   1        00-1B-FC-0E-34-3E    16400
1722   1        00-E0-18-45-C7-28 * 16400
4084   1        00-0E-A6-11-7C-5F * 16463
4084   1        00-17-31-B4-D2-57    16463
5941   1        00-05-5D-DB-BA-7A    16482
5941   1        00-13-D4-9A-FB-08 * 16482

DES-1228/ME:4#
```

**disable flood\_fdb**

Purpose	Used to disable flooding MAC function.
Syntax	<b>disable flood_fdb</b>
Description	The disable flood_fdb command is used to disable flooding MAC function.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable flood\_fdb:

```
DES-1228/ME:4#disable flood_fdb
Command: disable flood_fdb

Success.

DES-1228/ME:4#
```

**clear flood\_fdb**

Purpose	Used to clear the flooding database.
Syntax	<b>clear flood_fdb</b>
Description	Clear the flooding database.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To clear flood\_fdb:

```
DES-1228/ME:4#clear flood_fdb
```

```
Command: clear flood_fdb
```

```
Success.
```

```
DES-1228/ME:4#
```

**create auto\_fdb**

Purpose	Used to discover (VLAN, MAC, Port) for specified IP address and automatically created onto FDB.
Syntax	<b>create auto_fdb &lt; ipaddr &gt;</b>
Description	The create auto_fdb command is used to create IP address entry onto auto FDB. The device will discover (VLAN, MAC, Port) for specified IP address and automatically created onto FDB as static.
Parameters	< ipaddr > - The user can enter an IP address here.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create auto\_fdb:

```
DES-1228/ME:4#create auto_fdb 10.90.90.10
```

```
Command: create auto_fdb 10.90.90.10
```

```
Success.
```

```
DES-1228/ME:4#
```

**show auto\_fdb**

Purpose	Used to show the auto FDB.
Syntax	<b>show auto_fdb {&lt; ipaddr &gt;}</b>
Description	The show auto_fdb command is showed the auto FDB.
Parameters	< ipaddr > - The user can enter an IP address here.
Restrictions	None.

Example usage:

To show auto\_fdb:

```
DES-1228/ME:4#show auto_fdb 10.90.90.10
```

```
Command: show auto_fdb 10.90.90.10
```

```
IP Address      VLAN ID MAC Address      Port Time Stamp
-----
10.90.90.10
```

```
DES-1228/ME:4#
```

## delete auto\_fdb

Purpose	Use to delete specified IP address entry.
Syntax	<b>delete auto_fdb &lt; ipaddr &gt;</b>
Description	The delete auto_fdb command is used to delete specified IP address entry from auto FDB.
Parameters	< ipaddr > - The user can enter an IP address here.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete auto\_fdb:

```
DES-1228/ME:4#delete auto_fdb 10.90.90.10
```

```
Command: delete auto_fdb 10.90.90.10
```

```
Success.
```

```
DES-1228/ME:4#
```

## BROADCAST STORM CONTROL COMMANDS

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

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the **Drop** option of the **Action** field in the table below. The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the CountDown field. If this field times out and the packet storm continues, the port will be placed in a Rest mode which will produce a warning message to be sent to the Trap Receiver. Once in Rest mode, the only methods of recovering this port are (1) auto-recovery after 5 minutes or (2) to manually recoup it using the **Port Configuration** window in the **Administration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the **Shutdown** option of the **Action** field in the table below.

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

Command	Parameters
config traffic control	[ <portlist>   all ] { broadcast [enable disable]   multicast [enable disable]   unicast [enable disable]   action [drop   shutdown]   threshold <value 64-1000000>   time_interval <secs 5-30>   countdown [<minutes 0>   <minutes 5-30>] }(1)
show traffic control	{<portlist>}
config traffic trap	[none   storm_occurred   storm_cleared   both]

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

### config traffic control

Purpose	Used to configure broadcast/multicast/unicast packet storm control. The software mechanism is provided to monitor the traffic rate in addition to the hardware storm control mechanism previously provided.
Syntax	<b>config traffic control [ &lt;portlist&gt;   all ] { broadcast [enable disable]   multicast [enable disable]   unicast [enable disable]   action [drop   shutdown]   threshold &lt;value 64-1000000&gt;   time_interval &lt;secs 5-30&gt;   countdown [&lt;minutes 0&gt;   &lt;minutes 5-30&gt;] }(1)</b>
Description	This command is used to configure broadcast/multicast/unicast storm control. By adding the new software traffic control mechanism, the user can now use both a hardware and software mechanism, the latter of which will now provide shutdown, recovery and trap notification functions for the Switch.
Parameters	<p>&lt;portlist&gt; – Used to specify a range of ports to be configured for traffic control.</p> <p>all – Specifies all ports are to be configured for traffic control on the Switch.</p> <p>broadcast [enable   disable] – Enables or disables broadcast storm control.</p> <p>multicast [enable   disable] – Enables or disables multicast storm control.</p> <p>unicast [enable   disable] – Enables or disables Unknown unicast traffic control.</p> <p>action – Used to configure the action taken when a storm control has been detected on the Switch. The user has two options:</p> <p style="padding-left: 20px;">drop – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.</p> <p style="padding-left: 20px;">shutdown – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to</p>

## config traffic control

the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Storm continues, the port will be placed in Rest mode and is no longer operational until (1) auto-recovery after 5 minutes or (2) the user manually resets the port using the **config ports 1 state disable** and **config ports 1 state enable** command. Choosing this option obligates the user to configure the *time\_interval* field as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.

*threshold <value 64-1000000>* – The upper threshold at which the specified traffic control is switched on. The *<value>* is the number of broadcast/multicast/Unknown unicast packets, in Kbits per second (Kbit/sec), received by the Switch that will trigger the storm traffic control measures. The default setting is 64 Kbit/sec.

*time\_interval* – The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value.

*secs 5-30* – The Interval may be set between 5 and 30 seconds with the default setting of 5 seconds.

*countdown* – The countdown timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as **shutdown** in the **action** field of this command and therefore will not operate for Hardware based Traffic Control implementations.

*minutes 0* – 0 is the default setting for this field and 0 will denote that the port will never shutdown.

*minutes 5-30* – Select a time from 5 to 30 minutes that the Switch will wait before shutting down. Once this time expires and the port is still experiencing packet storms, the port will be placed in rest mode and can only be manually recovered using the config ports command mentioned previously in this manual.

Restrictions Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4# config traffic control 1-12 broadcast enable action shutdown threshold
64 countdown 10 time_interval 10
```

```
Command: config traffic control 1-12 broadcast enable action shutdown threshold 64
countdown 10 time_interval 10
```

Success.

```
DES-1228/ME:4#
```

## show traffic control

Purpose	Used to display current traffic control settings.
Syntax	<b>show traffic control { &lt;portlist&gt; }</b>
Description	This command displays the current storm traffic control configuration on the Switch.
Parameters	<i>&lt;portlist&gt;</i> – Used to specify port or list of ports for which to display traffic control settings. The beginning and end of the port list range are separated by a dash.
Restrictions	None.



Example usage:

To display traffic control setting for ports 1-4:

```
DES-1228/ME:4#show traffic control 1-4
Command: show traffic control 1-4

Traffic Storm Control Trap :[None]

Port Thres Broadcast Multicast Unicast Action Count Time
  hold Storm Storm Storm down Interval
-----
1 64 Disabled Disabled Disabled drop 0 5
2 64 Disabled Disabled Disabled drop 0 5
3 64 Disabled Disabled Disabled drop 0 5
4 64 Disabled Disabled Disabled drop 0 5

Total Entries : 4

DES-1228/ME:4#
```

## config traffic trap

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

Example usage:

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

```
DES-1228/ME:4# config traffic trap both
Command: config traffic trap both

Success.

DES-1228/ME:4#
```

## CoS COMMANDS

The DES-1228/ME supports 802.1p priority queuing. The Switch has four priority queues. These priority queues are numbered from 3 (Class 3) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

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

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

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

Command	Parameters
config bandwidth_control	<portlist> {rx_rate [ no_limit   <value 64-1024000>]   tx_rate [ no_limit   <value 64-1024000>]}(1)
show bandwidth_control	<portlist>
config scheduling	<class_id 0-3> {weight <value 1-55>}
config scheduling_mechanism	[strict   weight_fair]
show scheduling	
show scheduling_mechanism	
config 802.1p user_priority	<priority 0-7> <class_id 0-3>
show 802.1p user_priority	
config 802.1p default_priority	[<portlist>   all] <priority 0-7>
show 802.1p default_priority	<portlist>
config cos mapping port	[<portlist>   all] [none {port_mapping   ethernet [802.1p   mac_mapping]   ip [tos   dscp]}](1)
show cos mapping	{port <portlist> }
config cos port_mapping	class [ 0   3 ] port [<portlist>   all]
show cos port_mapping	{port <portlist> }
config cos mac_mapping	destination_addr <macaddr> [class <class_id 0-3>]
show cos mac_mapping	{destination_addr < macaddr > }
config cos tos value	<value 0-7> [class <class_id 0-3>]
show cos tos	{value <value 0-7>}
config dscp_mapping	dscp_value <value 0-63> [class <class_id 0-3>]
show dscp_mapping	{dscp_value <value 0-63> }

Command	Parameters
config mgmt_pkt_priority	[default   <priority 0-7>]
show mgmt_pkt_priority	

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

## config bandwidth\_control

Purpose	Used to configure bandwidth control on a port by-port basis.
Syntax	<b>config bandwidth_control &lt;portlist&gt; {rx_rate [ no_limit   &lt;value 64-1024000&gt;]   tx_rate [ no_limit   &lt;value 64-1024000&gt;]}(1)</b>
Description	The <b>config bandwidth_control</b> command is used to configure bandwidth on a port by-port basis.
Parameters	<p><i>&lt;portlist&gt;</i> – Specifies a port or range of ports to be configured.</p> <p><i>rx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <i>&lt;value 64-1024000&gt;</i>) will be applied to the rate at which the above specified ports will be allowed to receive packets</p> <ul style="list-style-type: none"> <li>▪ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports.</li> <li>▪ <i>&lt;value 64-1024000&gt;</i> – Specifies the traffic limit, in Kbits, that the above ports will be allowed to receive.</li> </ul> <p><i>tx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <i>&lt;value 64-1024000&gt;</i>) will be applied to the rate at which the above specified ports will be allowed to transmit packets.</p> <ul style="list-style-type: none"> <li>▪ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports.</li> <li>▪ <i>&lt;value 64-1024000&gt;</i> – Specifies the traffic limit, in Kbits, that the above ports will be allowed to receive.</li> </ul>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DES-1228/ME:4#config bandwidth_control 1 rx_rate 64
```

```
Command: config bandwidth_control 1 rx_rate 64
```

**Note:** To perform precise bandwidth control, it is required to enable the flow control to mitigate the retransmission of TCP traffic.

Success.

```
DES-1228/ME:4#
```

## show bandwidth\_control

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

Example usage:

To display bandwidth control settings:

```
DES-1228/ME:4#show bandwidth_control 1-5
```

```
Command: show bandwidth_control 1-5
```

#### Bandwidth Control Table

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1	no_limit	no_limit	no_limit	no_limit
2	no_limit	no_limit	no_limit	no_limit
3	no_limit	no_limit	no_limit	no_limit
4	no_limit	no_limit	no_limit	no_limit
5	no_limit	no_limit	no_limit	no_limit

```
DES-1228/ME:4#
```

## config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	<b>config scheduling &lt;class_id 0-3&gt; [weight &lt;value 1-55&gt;]</b>
Description	<p>The Switch contains four hardware priority queues. Incoming packets must be mapped to one of these four queues. This command is used to specify the rotation by which these four hardware priority queues are emptied.</p> <p>The Switch's default (if the config scheduling command is not used) is to empty the four hardware priority queues in order – from the highest priority queue (hardware queue 3) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.</p> <p>weight &lt;value 1-55&gt; – Specifies the weights for weighted COS queuing. A value between 1 and 55 can be specified.</p>
Parameters	<class_id 0-3> – This specifies which of the four hardware priority queues the <b>config scheduling</b> command will apply to. The four hardware priority queues are identified by number – from 0 to 3 – with the 0 queue being the lowest priority.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each queue:

```
DES-1228/ME:4# config scheduling 0 weight 55
```

```
Command: config scheduling 0 weight 55
```

```
Success.
```

```
DES-1228/ME:4#
```

## show scheduling

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

Example usage:

To display the current scheduling configuration:

```
DES-1228/ME:4#show scheduling
```

```
Command: show scheduling
```

### QoS Output Scheduling

Class ID	Weight
-----	-----
Class-0	1
Class-1	2
Class-2	4
Class-3	8

```
DES-1228/ME:4#
```

## config scheduling\_mechanism

Purpose	Used to configure the scheduling mechanism for the QoS function
Syntax	<b>config scheduling_mechanism [strict   weight_fair]</b>
Description	<p>The <b>config scheduling_mechanism</b> command allows the user to select between a <b>weight fair</b> and a <b>Strict</b> mechanism for emptying the priority classes of service of the QoS function. The Switch contains seven hardware priority classes of service. Incoming packets must be mapped to one of these seven hardware priority classes of service. This command is used to specify the rotation by which these seven hardware priority classes of service are emptied.</p> <p>The Switch's default is to empty the seven priority classes of service in order – from the highest priority class of service (queue 6) to the lowest priority class of service (queue 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority class of service to transmit its packets. Lower classes of service will be pre-empted from emptying its queue if a packet is received on a higher class of service. The packet that was received on the higher class of service will transmit its packet before allowing the lower class to resume clearing its queue.</p>
Parameters	<p><i>strict</i> – Entering the <i>strict</i> parameter indicates that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin.</p> <p><i>weight_fair</i> – Entering the <i>weight fair</i> parameter indicates that the priority classes of service will empty packets in a fair weighted order. That is to say that they will be emptied in an even distribution.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each QoS queue:

```
DES-1228/ME:4#config scheduling_mechanism strict
```

```
Command: config scheduling_mechanism strict
```

Note: The strict mode is only supported at the highest queue and the other lower queues will still work at WRR mode.

Success.

```
DES-1228/ME:4#
```

## show scheduling\_mechanism

Purpose	Used to display the current traffic scheduling mechanisms in use on the Switch.
Syntax	<b>show scheduling_mechanism</b>
Description	This command will display the current traffic scheduling mechanisms in use on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the scheduling mechanism:

```
DES-1228/ME:4#show scheduling_mechanism
```

```
Command: show scheduling_mechanism
```

```
QOS Scheduling_mechanism
```

```
CLASS ID  Mechanism
-----  -
Class-0   weight_fair
Class-1   weight_fair
Class-2   weight_fair
Class-3   strict
```

```
DES-1228/ME:4#
```

**config 802.1p user\_priority**

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the four hardware queues available on the Switch.																											
Syntax	<b>config 802.1p user_priority &lt;priority 0-7&gt; &lt;class_id 0-3&gt;</b>																											
Description	<p>This command allows users to configure the way the Switch will map an incoming packet, based on its 802.1p user priority, to one of the four available hardware priority queues on the Switch.</p> <p>The Switch's default is to map the following incoming 802.1p user priority values to the four hardware priority queues:</p> <table border="1"> <thead> <tr> <th>802.1p</th> <th>Hardware Queue</th> <th>Remark</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>1</td> <td>Mid-low</td> </tr> <tr> <td>1</td> <td>0</td> <td>Lowest</td> </tr> <tr> <td>2</td> <td>0</td> <td>Lowest</td> </tr> <tr> <td>3</td> <td>1</td> <td>Mid-low</td> </tr> <tr> <td>4</td> <td>2</td> <td>Mid-high</td> </tr> <tr> <td>5</td> <td>2</td> <td>Mid-high</td> </tr> <tr> <td>6</td> <td>3</td> <td>Highest</td> </tr> <tr> <td>7</td> <td>3</td> <td>Highest.</td> </tr> </tbody> </table> <p>This mapping scheme is based upon recommendations contained in IEEE 802.1D. Change this mapping by specifying the 802.1p user priority users want to map to the &lt;class_id 0-3&gt; (the number of the hardware queue).</p> <p>&lt;priority 0-7&gt; – The 802.1p user priority to associate with the &lt;class_id 0-3&gt; (the number of the hardware queue).</p> <p>&lt;class_id 0-3&gt; – The number of the Switch's hardware priority queue. The Switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).</p>	802.1p	Hardware Queue	Remark	0	1	Mid-low	1	0	Lowest	2	0	Lowest	3	1	Mid-low	4	2	Mid-high	5	2	Mid-high	6	3	Highest	7	3	Highest.
802.1p	Hardware Queue	Remark																										
0	1	Mid-low																										
1	0	Lowest																										
2	0	Lowest																										
3	1	Mid-low																										
4	2	Mid-high																										
5	2	Mid-high																										
6	3	Highest																										
7	3	Highest.																										
Restrictions	Only Administrator-level users can issue this command.																											

Example usage:

To configure 802.1p user priority on the Switch:

```
DES-1228/ME:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DES-1228/ME:4#
```

**show 802.1p user\_priority**

Purpose	Used to display the current mapping between an incoming packet's 802.1p priority value and one of the Switch's four hardware priority queues.
Syntax	<b>show 802.1p user_priority</b>
Description	The <b>show 802.1p user_priority</b> 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-1228/ME:4# show 802.1p user_priority
```

```
Command: show 802.1p user_priority
```

#### QOS Class of Traffic

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

```
DES-1228/ME:4#
```

## config 802.1p default\_priority

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

Example usage:

To configure 802.1p default priority on the Switch:

```
DES-1228/ME:4#config 802.1p default_priority all 5
```

```
Command: config 802.1p default_priority all 5
```

```
Success.
```

```
DES-1228/ME:4#
```

## show 802.1p default\_priority

Purpose	Used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Syntax	<b>show 802.1p default_priority</b> {<portlist>}
Description	The <b>show 802.1p default_priority</b> command displays the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Parameters	<portlist> – Specifies a port or range of ports to be configured.
Restrictions	None.

Example usage:



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

```
DES-1228/ME:4# show 802.1p default_priority
Command: show 802.1p default_priority

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

DES-1228/ME:4#
```

## config cos mapping

Purpose	Used to configure the CoS to port mapping method to be used on the switch.
Syntax	<b>config cos mapping port</b> [ <b>&lt;portlist&gt;</b>   <b>all</b> ] [ <b>none</b>   <b>{port_mapping   ethernet [802.1p   mac_mapping]   ip [tos   dscp]}</b> ](1)]
Description	The <b>config cos mapping</b> is used to set the method of which incoming packets will be identified for the CoS to port mapping feature on the Switch. Identified packets will be forwarded to the appropriate CoS queue.
Parameters	<p><i>&lt;portlist&gt;</i> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Specifies all ports will be configured.</p> <p><i>none</i> – Disable all priority-base CoS features.</p> <p><i>port_mapping</i> – Enable port-based CoS.</p> <p><i>ethernet</i> – Enable Ethernet frame based priority.</p> <p><i>802.1p</i> – Enable 802.1p CoS</p> <p><i>mac_mapping</i> – Enable MAC-based CoS.</p> <p><i>ip</i> – Enable Ethernet frame based priority.</p>
Restrictions	None.

Example usage:

To configure port 1 as a CoS enabled port which uses the physical port number as its criteria for identifying packets:

```
DES-1228/ME:4#config cos mapping port 1 port_mapping
Command: config cos mapping port 1 port_mapping

Success.

DES-1228/ME:4#
```

## show cos mapping

Purpose	Used to show CoS mapping.
Syntax	<b>show cos mapping</b> { <b>port &lt;portlist&gt;</b> }
Description	The <b>show cos mapping</b> displays information regarding CoS mapping enabled ports and their mapping method.
Parameters	<i>&lt;portlist&gt;</i> – Specifies a range of ports to be displayed. If no parameter is specified, the all ports priority settings will be shown.
Restrictions	None.

Example usage:

To show the CoS mapping information:

```
DES-1228/ME:4# show cos mapping
Command: show cos mapping

Port      Port_priority      Ethernet_priority      IP_priority
-----
1         off                802.1p                 off
2         off                802.1p                 off
3         off                802.1p                 off
4         off                802.1p                 off
5         off                802.1p                 off
```

6	off	802.1p	off
7	off	802.1p	off
8	off	802.1p	off
9	off	802.1p	off
10	off	802.1p	off
11	off	802.1p	off
12	off	802.1p	off
13	off	802.1p	off
14	off	802.1p	off
15	off	802.1p	off
16	off	802.1p	off
17	off	802.1p	off
18	off	802.1p	off
19	off	802.1p	off
20	off	802.1p	off

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

## config cos port\_mapping

Purpose	Used to map a specific port to one of the hardware queues available on the switch.
Syntax	<b>config cos port_mapping class [ 0   3 ] port [&lt;portlist&gt;   all]</b>
Description	The config cos port_mapping command is used to configure port-to-class CoS mapping.
Parameters	<p>0-3 – The number of the switch's hardware priority queue. The switch has eight hardware priority queues available. They are numbered between 0 (the lowest priority queue) and 3 (the highest priority queue).</p> <p>&lt;portlist&gt; – Specifies a port or range of ports to be configured.</p> <p>all – To set all ports in the system at once, you may use the "all" parameter.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a specific CoS queue to be mapped to a destination port 1:

```
DES-1228/ME:4# config cos port_mapping class 3 port 1
Command: config cos port_mapping class 3 port 1
```

Success.

```
DES-1228/ME:4#
```

## show cos port\_mapping

Purpose	Used to map the destination MAC address in incoming packets to one of the hardware queues available on the switch.
Syntax	<b>show cos port_mapping {port &lt;portlist&gt;}</b>
Description	The <b>show cos mac_mapping</b> command is used to view map static destination MAC addresses to one of the CoS traffic classes.
Parameters	<portlist> – Specifies a port or range of ports to be configured. If no parameter is specified, all port-to-class mappings will be shown.
Restrictions	None.

Example usage:

To show the cos port\_mapping of the port 3:

```
DES-1228/ME:4# show cos port_mapping port 3
Command: show cos port_mapping port 3

Port  Priority
-----
 3      3

DES-1228/ME:4#
```

## config cos mac\_mapping

Purpose	Used to map the destination MAC address in incoming packet to one of the hardware queues available on the switch.
Syntax	<b>config cos mac_mapping destination_addr &lt;macaddr&gt; [class &lt;class_id 0-3&gt;]</b>
Description	The <b>config cos mac_mapping</b> command is used to map static destination MAC address to one of the traffic classes.
Parameters	<i>destination_addr</i> – The MAC address to be configured. <class_id 0-3> – The number of the Switch's hardware priority queue. The Switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the destination MAC address 00-01-02-03-04-05 to traffic class 2 mapping:

```
DES-1228/ME:4# config cos mac_mapping destination_addr 00-01-02-03-04-05 class 2
Command: config cos mac_mapping destination_addr 00-01-02-03-04-05 class 2

Success.

DES-1228/ME:4#
```

## show cos mac\_mapping

Purpose	Used to show the mapping between destination MAC addresses and CoS traffic classes.
Syntax	<b>show cos mac_mapping {destination_addr &lt;macaddr&gt;}</b>
Description	The <b>show cos mac_mapping</b> command display the information of the destination MAC address mapped to a traffic class.
Parameters	<i>destination_addr</i> – The MAC address of the incoming packet destination address. If no parameter is specified, all the MAC address mapping to traffic class will be shown.
Restrictions	None.

Example usage:

To show the MAC address to traffic class mapping of MAC address 00-01-02-03-04-05:

```
DES-1228/ME:4# show cos mac_mapping destination_addr 00-01-02-03-04-05
```

```
Command: show cos mac_mapping destination_addr 00-01-02-03-04-05
```

MAC Address	Class
-----	
00-01-02-03-04-05	2

```
DES-1228/ME:4#
```

## config cos tos value

Purpose	Used to map the ToS value in the IP header of incoming packets to one of the eight hardware queues available on the switch.
Syntax	<b>config cos tos value &lt;value 0-7&gt; [class &lt;class_id 0-3&gt;]</b>
Description	The <b>config cos tos</b> command is used to configure ToS to traffic class mapping.
Parameters	<i>&lt;value 0-7&gt;</i> – The ToS value of incoming packet that you want to associate with the traffic class.  <i>&lt;class_id 0-3&gt;</i> – The number of the Switch's hardware priority queue. The Switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

Configure the TOS 5 to the traffic class 1 mapping:

```
DES-1228/ME:4# config cos tos value 5 class 1
```

```
Command: config cos tos value 5 class 1
```

```
Success.
```

```
DES-1228/ME:4#
```

## show cos tos

Purpose	Used to show TOS value to traffic class mapping.
Syntax	<b>show cos tos {value &lt;value 0-7&gt;}</b>
Description	The <b>show cos tos</b> command displays the information of ToS to traffic class mappings.
Parameters	<value 0-7> – The TOS value of the incoming packet. If no parameter is specified, all the ToS values to traffic class mappings will be shown.
Restrictions	None.

Example usage:

To show the TOS to traffic class mapping of the TOS 5:

```
DES-1228/ME:4# show cos tos value 5
```

```
Command: show cos tos value 5
```

```
TOS value          Class
-----
5                  2
```

```
DES-1228/ME:4#
```

## config dscp\_mapping

Purpose	Used to map the DSCP value in the IP header of incoming packet to one of the four hardware queues available on the switch.
Syntax	<b>config dscp_mapping dscp_value &lt;value 0-63&gt; [class &lt;class_id 0-3&gt;]</b>
Description	The <b>config dscp_mapping</b> command is used to configure DSCP mapping to traffic class. This command is supported when the ACL commands are not supported.
Parameters	<value 0-63> – The DSCP value of the incoming packet you want to associate with the class_id.  <class_id 0-3> – The number of the Switch's hardware priority queue. The switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DSCP map to traffic class:

```
DES-1228/ME:4# config dscp_mapping dscp_value 8 class 1
```

```
Command: config dscp_mapping dscp_value 8 class 1
```

```
Success.
```

```
DES-1228/ME:4#
```

## show dscp\_mapping

Purpose	Used to show DSCP value map to traffic class.
Syntax	<b>show dscp_mapping {dscp_value &lt;value 0-63&gt;}</b>
Description	The <b>show dscp_mapping</b> command displays the information for DSCP mapping to traffic class. This command is supported when the ACL commands are not supported.
Parameters	<value 0-63> – The DSCP value of the incoming packet. If no parameter is specified, all the DSCP value mapping to traffic class will be shown.
Restrictions	None.

Example usage:

To show the DSCP map to traffic class:

```
DES-1228/ME:4# show dscp_mapping
Command: show dscp_mapping

DSCP      Class
-----
0          0
1          0
2          0
3          0
4          0
5          0
6          0
7          0
8          0
9          0
10         0
11         0
12         0
13         0
14         0
15         0
16         0
17         0
18         0
19         0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

**config mgmt\_pkt\_priority**

Purpose	This command is used to configure the management packet priority of the Switch.
Syntax	<b>config mgmt_pkt_priority [default   &lt;priority 0-7&gt;]</b>
Description	This command is used to configure the management packet priority of the Switch.
Parameters	<i>default</i>   <i>&lt;priority 0-7&gt;</i> - This field specifies the default VLAN priority value
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default value to the management packet priority of the Switch:

```
DES-1228/ME:4#config mgmt_pkt_priority default
Command: config mgmt_pkt_priority default

Success.

DES-1228/ME:4#
```

**show mgmt\_pkt\_priority**

Purpose	This command is used to display the management packet priority of the Switch.
Syntax	<b>show mgmt_pkt_priority</b>
Description	This command is used to display the management packet priority of the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the default value to the management packet priority of the Switch:

```
DES-1228/ME:4#show mgmt_pkt_priority
Command: show mgmt_pkt_priority

Management Packet Priority : default

DES-1228/ME:4#
```



## PORT MIRRORING COMMANDS

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

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

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

### config mirror port

Purpose	Used to configure a mirror port – source port pair on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe can then be attached to study the traffic crossing the source port in a completely obtrusive manner.
Syntax	<b>config mirror port &lt;port&gt; {[add  delete] source ports &lt;portlist&gt; [rx tx both]}</b>
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, users can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	<p><b>&lt;port&gt;</b> – This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be operating at the same speed as the source port.</p> <p><b>[add   delete]</b> – Specifies if the user wishes to add or delete ports to be mirrored that are specified in the <i>source ports</i> parameter.</p> <p><b>source ports</b> – The port or ports being mirrored. This cannot include the Target port.</p> <p><b>&lt;portlist&gt;</b> – This specifies a port or range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port.</p> <p><b>rx</b> – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p><b>tx</b> – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p><b>both</b> – Mirrors all the packets received or sent by the port or ports in the port list.</p>
Restrictions	The Target port cannot be listed as a source port. Only Administrator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DES-1228/ME:4# config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

DES-1228/ME:4#
```

Example usage:

To delete the mirroring ports:

```
DES-1228/ME:4#config mirror port 1 delete source port 2-4 both
Command: config mirror 1 delete source 2-4 both

Success.

DES-1228/ME:4#
```

## enable mirror

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

Example usage:

To enable mirroring configurations:

```
DES-1228/ME:4#enable mirror
Command: enable mirror

Success.

DES-1228/ME:4#
```

## disable mirror

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

Example usage:

To disable mirroring configurations:

```
DES-1228/ME:4#disable mirror
Command: disable mirror

Success.

DES-1228/ME:4#
```

## show mirror

Purpose	Used to show the current port mirroring configuration on the Switch.
Syntax	<b>show mirror</b>
Description	This command displays the current port mirroring configuration on the Switch.
Parameters	None
Restrictions	None.

Example usage:

To display mirroring configuration:

```
DES-1228/ME:4#show mirror
```

```
Command: show mirror
```

```
Current Settings
```

```
Mirror Status   : Enabled
```

```
Target Port     : 1
```

```
Mirrored Port  :
```

```
                RX :
```

```
                TX : 5-7
```

```
DES-1228/ME:4#
```

## VLAN COMMANDS

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

Command	Parameters
create vlan	<vlan_name 32> {tag <vlanid 2-4094>   advertisement}
delete vlan	<vlan_name 32>
create vlan vlanid	<vidlist> {advertisement}
delete vlan vlanid	<vidlist>
config vlan vlanid	<vidlist> {[ add [ tagged   untagged   forbidden ]  delete ] <portlist>   advertisement [ enable   disable ]   name <vlan_name 32>}(1)
config vlan	<vlan_name 32> {[ add [ tagged   untagged   forbidden ]  delete ] <portlist>   advertisement [ enable   disable ]}(1)
config gvrp	[<portlist>   all] {state [enable   disable] ingress_checking [enable   disable]   acceptable_frame [tagged_only   admit_all] pvid <vlanid 1-4094>}(1)
enable gvrp	
disable gvrp	
show vlan	{[<vlan_name 32>   vlanid <vidlist>   ports <portlist>]}
show gvrp	<portlist>

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

### create vlan

Purpose	Used to create a VLAN on the Switch.
Syntax	<b>create vlan &lt;vlan_name 32&gt; {tag &lt;vlanid 2-4094&gt;   advertisement}</b>
Description	This command allows the user to create a VLAN on the Switch.
Parameters	<p>&lt;vlan_name 32&gt; – The name of the VLAN to be created.</p> <p>&lt;vlanid 2-4094&gt; – The VLAN ID of the VLAN to be created. Allowed values = 2-4094</p> <p>advertisement – Specifies that the VLAN is able to join GVRP. If this parameter is not set, the VLAN cannot be configured to have forbidden ports.</p>
Restrictions	Each VLAN name can be up to 32 characters. Up to 4094 static VLANs may be created per configuration. Only Administrator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DES-1228/ME:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DES-1228/ME:4#
```

### delete vlan

## delete vlan

Purpose	Used to delete a previously configured VLAN on the Switch.
Syntax	<b>delete vlan &lt;vlan_name 32&gt;</b>
Description	This command will delete a previously configured VLAN on the Switch.
Parameters	<vlan_name 32> – The VLAN name of the VLAN to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To remove the VLAN “v1”:

```
DES-1228/ME:4#delete vlan v1
```

```
Command: delete vlan v1
```

```
Success.
```

```
DES-1228/ME:4#
```

## config vlan

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	<b>config vlan &lt;vlan_name 32&gt; {[ add [ tagged   untagged   forbidden ]  delete ] &lt;portlist&gt;   advertisement [ enable   disable ]}(1)</b>
Description	This command allows the user to add ports to the port list of a previously configured VLAN. The user can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	<p>&lt;vlan_name 32&gt; – The name of the VLAN to which to add ports.</p> <p><i>add</i> – Entering the add parameter will add ports to the VLAN. There are three types of ports to add:</p> <ul style="list-style-type: none"> <li>• <i>tagged</i> – Specifies the additional ports as tagged.</li> <li>• <i>untagged</i> – Specifies the additional ports as untagged.</li> <li>• <i>forbidden</i> – Specifies the additional ports as forbidden</li> </ul> <p><i>delete</i> – Deletes ports from the specified VLAN.</p> <p>&lt;portlist&gt; – A port or range of ports to add to, or delete from the specified VLAN.</p> <p><i>advertisement [enable   disable]</i> – Enables or disables GVRP on the specified VLAN.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#config vlan v1 add tagged 4-8
```

```
Command: config vlan v1 add tagged 4-8
```

```
Success.
```

```
DES-1228/ME:4#
```

To delete ports from a VLAN:

```
DES-1228/ME:4#config vlan v1 delete 6-8
```

```
Command: config vlan v1 delete 6-8
```

```
Success.
```

DES-1228/ME:4#

## create vlan vlanid

Purpose	Used to create multiple VLANs by VLAN ID list on the switch.
Syntax	<b>create vlan vlanid &lt;vidlist&gt; { advertisement }</b>
Description	The create vlans by vlanid list command creates multiple VLANs on the switch.
Parameters	<vidlist> – Specifies a range of multiple VLAN IDs to be created. advertisement – Join GVRP or not. If not, the VLAN can't join dynamically.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create VLAN ID on the switch:

```
DES-1228/ME:4#create vlan vlanid 5 advertisement
Command: create vlan vlanid 5 advertisement

Success

DES-1228/ME:4#
```

## delete vlan vlanid

Purpose	Used to delete multiple VLANs by VLAN ID on the switch.
Syntax	<b>delete vlan vlanid &lt;vidlist&gt;</b>
Description	The delete vlan by vlan id list command deletes previously configured multiple VLANs on the switch.
Parameters	<vidlist> – Specifies a range of multiple VLAN IDs to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete VLAN ID on the switch:

```
DES-1228/ME:4#delete vlan vlanid 5
Command: delete vlan vlanid 5

Success

DES-1228/ME:4#
```

## config vlan vlanid

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	<b>config vlan vlanid &lt;vidlist&gt; {[ add [ tagged   untagged   forbidden ]  delete ] &lt;portlist&gt;   advertisement [ enable   disable ]   name &lt;vlan_name 32&gt;}(1)</b>
Description	The config vlan vlanid command allows you to add or delete ports of the port list of previously configured VLAN(s). You can specify the additional ports as being tagged, untagged or forbidden. The same port is allowed to be an untagged member port of multiple VLAN's. You can also specify if the ports will join GVRP or not with the <i>advertisement</i> parameter.

**config vlan vlanid**

	The <i>name</i> parameter allows you to specify the name of the VLAN that needs to be modified.
Parameters	<p><i>&lt;vidlist&gt;</i> – Specifies a range of multiple VLAN IDs to be configured.</p> <p><i>tagged</i> – Specifies the additional ports as tagged.</p> <p><i>untagged</i> – Specifies the additional ports as untagged.</p> <p><i>forbidden</i> – Specifies the additional ports as forbidden.</p> <p><i>&lt;portlist&gt;</i> – A range of ports to add to the VLAN.</p> <p><i>advertisement</i> – Entering the advertisement parameter specifies if the port should join GVRP or not. There are two parameters:</p> <p><i>enable</i> – Specifies that the port should join GVRP.</p> <p><i>Disable</i> – Specifies that the port should not join GVRP.</p> <p><i>name</i> – Entering the name parameter specifies the name of the VLAN to be modified.</p> <p><i>&lt;name&gt;</i> – Enter a name for the VLAN</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config vlan vlanid on the switch:

```
DES-1228/ME:4#config vlan vlanid 5 add tagged 7 advertisement enable name RG
Command: config vlan vlanid 5 add tagged 7 advertisement enable name RG

Success.

DES-1228/ME:4#
```

**config gvrp**

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

Example usage:

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

```
DES-1228/ME:4#config gvrp 1-4 state enable ingress_checking enable acceptable_frame
tagged_only pvid 2
Command: config gvrp 1-4 state enable ingress_checking enable acceptable_frame
```

```
tagged_only pvid 2
```

```
Success.
```

```
DES-1228/ME:4#
```

## enable gvrp

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

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DES-1228/ME:4#enable gvrp
```

```
Command: enable gvrp
```

```
Success.
```

```
DES-1228/ME:4#
```

## disable gvrp

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

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DES-1228/ME:4#disable gvrp
```

```
Command: disable gvrp
```

```
Success.
```

```
DES-1228/ME:4#
```

## show vlan

Purpose	Used to display the current VLAN configuration on the Switch
Syntax	<b>show vlan [&lt;vlan_name 32&gt;   vlanid &lt;vidlist&gt;   ports &lt;portlist&gt; ]</b>
Description	This command displays summary information about each VLAN including the VLAN ID, VLAN name, VLAN Type, the Tagging/Untagging status, and the Member/Non-member/Forbidden status of each port that is a member of the VLAN.



## show vlan

Parameters	<p>&lt;vlanid&gt; – Specifies a range of multiple VLAN IDs to be displayed.</p> <p>&lt;ports&gt; – Specifies the ports to be displayed.</p> <p>&lt;vlan_name 32&gt; – The VLAN name of the VLAN for which to display a summary of settings.</p> <p>&lt;portlist&gt; – Specifies a port or range of ports that will be displayed.</p>
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DES-1228/ME:4#show vlan
Command: show vlan
VID          : 1          VLAN Name     : default
VLAN Type    : Static    Advertisement : Enabled
Member Ports : 1-28
Static Ports : 1-28
Current Tagged Ports :
Current Untagged Ports : 1-28
Static Tagged Ports :
Static Untagged Ports : 1-28
Forbidden Ports :

Total Entries : 1

DES-1228/ME:4#
```

To display the Switch's current VLAN settings for a specific port:

```
DES-1228/ME:4# DES-1228/ME:4#show vlan port 1
Command: show vlan ports 1

Port 1
VLAN ID  Untagged  Tagged  Forbidden  Dynamic
-----  -
1         X         -         -         -

DES-1228/ME:4#
```

## show gvrp

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

Example usage:

To display GVRP port status:

```
DES-1228/ME:4#show gvrp 1-10
```

```
Command: show gvrp 1-10
```

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

```
Total Entries : 10
```

## LINK AGGREGATION COMMANDS

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

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

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

### create link\_aggregation

Purpose	Used to create a link aggregation group on the Switch.
Syntax	<b>create link_aggregation group_id &lt;value 1-6&gt; {type[lacp   static]}</b>
Description	This command will create a link aggregation group with a unique identifier.
Parameters	<p>&lt;value&gt; – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p>type – Specify the type of link aggregation used for the group. If the type is not specified the default type is <i>static</i>.</p> <p>1.0 <i>lacp</i> – 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.</p> <p>2.0 <i>static</i> – 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 trunk 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.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DES-1228/ME:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.
DES-1228/ME:4#
```

### delete link\_aggregation group\_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	<b>delete link_aggregation group_id &lt;value 1-6&gt;</b>

## delete link\_aggregation group\_id

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

Example usage:

To delete link aggregation group:

```
DES-1228/ME:4#delete link_aggregation group_id 6
```

```
Command: delete link_aggregation group_id 6
```

```
Success.
```

```
DES-1228/ME:4#
```

## config link\_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	<b>config link_aggregation group_id &lt;value 1-6&gt;{master_port &lt;port&gt;   ports &lt;portlist&gt;   state [enable disable]}(1)</b>
Description	This command allows users to configure a link aggregation group that was created with the <b>create link_aggregation</b> command above.
Parameters	<p><i>group_id</i> &lt;value 1-6&gt; – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>master_port</i> &lt;port&gt; – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.</p> <p><i>ports</i> &lt;portlist&gt; – Specifies a port or range of ports that will belong to the link aggregation group.</p> <p><i>state</i> [enable   disable] – Allows users to enable or disable the specified link aggregation group.</p>
Restrictions	Only Administrator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

To define a load-sharing group of ports, group-id 1, master port 1 with group members ports 1 through 4:

```
DES-1228/ME:4#config link_aggregation group_id 1 master_port 1 ports 1-4
```

```
Command: config link_aggregation group_id 1 master_port 1 ports 1-4
```

```
Success.
```

```
DES-1228/ME:4#
```

## config link\_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
Syntax	<b>config link_aggregation algorithm [mac_source   mac_destination   mac_source_dest ]</b>
Description	This command configures the part of the packet examined by the Switch when selecting the egress port for transmitting load-sharing data. This feature is only available using the

## config link\_aggregation algorithm

	address-based load-sharing algorithm.
Parameters	<p><i>mac_source</i> – Indicates that the Switch should examine the MAC source address.</p> <p><i>mac_destination</i> – Indicates that the Switch should examine the MAC destination address.</p> <p><i>mac_source_dest</i> – Indicates that the Switch should examine the MAC source and destination addresses</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#config link_aggregation algorithm mac_source_dest
```

```
Command: config link_aggregation algorithm mac_source_dest
```

```
Success.
```

```
DES-1228/ME:4#
```

## show link\_aggregation

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

Example usage:

To display Link Aggregation configuration:

```
DES-1228/ME:4#show link_aggregation
```

```
Command: show link_aggregation
```

```
Link Aggregation Algorithm = MAC-source-dest
```

```

Group ID      : 1
Master Port   : 1
Member Port   : 1, 5-10
Active Port   :
Status        : Disabled
Flooding Port : 0

```

```
DES-1228/ME:4#
```

## config lacp\_ports

Purpose	Used to configure settings for LACP compliant ports.
---------	--

**config lacp\_ports**

Syntax	<b>config lacp_ports &lt;portlist&gt; mode [active   passive]</b>
Description	This command is used to configure ports that have been previously designated as LACP ports (see <b>create link_aggregation</b> ).
Parameters	<p><i>&lt;portlist&gt;</i> – Specifies a port or range of ports to be configured.</p> <p><i>mode</i> – Select the mode to determine if LACP ports will process LACP control frames.</p> <ul style="list-style-type: none"> <li>• <i>active</i> – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be 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.</li> <li>• <i>passive</i> – 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).</li> </ul>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DES-1228/ME:4#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DES-1228/ME:4#
```

**show lacp\_port**

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

Example usage:

To display LACP port mode settings:

```
DES-1228/ME:4#show lacp_port 1-10
```

```
Command: show lacp_port 1-10
```

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

```
DES-1228/ME:4#
```

## BASIC IP COMMANDS

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

Command	Parameters
config ipif	[System] [{ <i>ipaddress</i> <network_address>   <i>vlan</i> <vlan_name 32>   <i>state</i> [enable disable]}   <i>bootp</i>   <i>dhcp</i>   <i>dhcp_option12</i> [ <i>hostname</i> <hostname 63>   <i>clear_hostname</i>   <i>state</i> [enable disable]]]
show ipif	
enable autoconfig*	

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

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

### config ipif

Purpose	Used to configure the System IP interface.
Syntax	<b>config ipif [System] [{ <i>ipaddress</i> &lt;network_address&gt;   <i>vlan</i> &lt;vlan_name 32&gt;   <i>state</i> [enable disable]}   <i>bootp</i>   <i>dhcp</i>   <i>dhcp_option12</i> [<i>hostname</i> &lt;hostname 63&gt;   <i>clear_hostname</i>   <i>state</i> [enable disable]]]</b>
Description	This command is used to configure the System IP interface on the Switch.
Parameters	<p><i>System</i> – Enter System.</p> <p><i>ipaddress</i> &lt;network_address&gt; – IP address and netmask of the IP interface to be created. Users can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format 10.1.2.3/8).</p> <p>&lt;<i>vlan_name</i> 32&gt; – The name of the VLAN corresponding to the System IP interface.</p> <p><i>state</i> [enable   disable] – Allows users to enable or disable the IP interface.</p> <p><i>bootp</i> – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface.</p> <p><i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface. If users are using the autoconfig feature, the Switch becomes a DHCP client automatically so it is not necessary to change the ipif settings.</p> <p><i>dhcp_option12</i> [<i>hostname</i> &lt;hostname 63&gt; – Allows users to specify the option12 hostname.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DES-1228/ME:4#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DES-1228/ME:4#
```



**show ipif**

Purpose	Used to display the configuration of an IP interface on the Switch.
Syntax	<b>show ipif</b>
Description	This command will display the configuration of an IP interface on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display IP interface settings.

```
DES-1228/ME:4#show ipif
Command: show ipif

IP Interface Settings

Interface Name      : System
IP Address         : 192.168.69.123 (MANUAL)
Subnet Mask        : 255.255.255.0
VLAN Name          : default
Admin. State       : Enabled
Link Status        : Link DOWN
Member Ports       : 1-28
DHCP Option12 State : Disabled
DHCP Option12 Host Name :

Total Entries   : 1

DES-1228/ME:4#
```

**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	<b>enable autoconfig</b>
Description	When autoconfig is enabled on the Switch, the DHCP reply will contain a configuration file and path name. It will then request the file from the TFTP server specified in the reply. When autoconfig is enabled, the ipif settings will automatically become DHCP client.
Parameters	None.
Restrictions	When autoconfig is enabled, the Switch becomes a DHCP client automatically (same as: config ipif System dhcp). The DHCP server must have the TFTP server IP address and configuration file name, and be configured to deliver this information in the data field of the DHCP reply packet. The TFTP server must be running and have the requested configuration file in its base directory when the request is received from the Switch. Consult the DHCP server and TFTP server software instructions for information on loading a boot file or configuration file. Only Administrator-level users can issue this command.

Example usage:

To enable auto configuration on the Switch:

```
DES-1228/ME:4#enable autoconfig
```

```
Command: enable autoconfig
```

```
Success.
```

```
DES-1228/ME:4#
```



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

## IGMP SNOOPING COMMANDS

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

Command	Parameters
config igmp_snooping	[ vlan_name <vlan_name 32>  all] {host_timeout <sec 1-16711450>   router_timeout <sec 1-16711450>   leave_timer <sec 1-16711450>   state [enable disable]   fast_leave [enable disable]}(1)
config igmp_snooping querier	[ vlan_name <vlan_name 32>  all] {query_interval <sec 1-65535>   max_response_time <sec 1-25>   robustness_variable <value 1-255>  last_member_query_interval <sec 1-25>   state [enable disable]}(1)
config router_ports	<vlan_name 32> [add   delete] <portlist>
config router_port_forbidden	<vlan_name 32> [add   delete] <portlist>
enable igmp snooping	{forward_mcrouter_only}
show igmp snooping	{vlan <vlan_name 32> }
disable igmp snooping	{forward_mcrouter_only}
show router ports	{vlan <vlan_name 32>} {[static   dynamic   forbidden]}
show igmp_snooping forwarding	{vlan <vlan_name 32>}
show igmp_snooping group	{vlan <vlan_name 32>} {data_driven}
config igmp snooping data_driven_learning	[ vlan_name <vlan_name 32>  all] {aged_out [enable disable]}(1)
config igmp_snooping data_driven_learning max_learned_entry	<value 1-64>
clear igmp snooping data_driven_group	[ vlan_name <vlan_name 32>   all ]

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

### config igmp\_snooping

Purpose	Used to configure IGMP snooping on the Switch.
Syntax	<b>config igmp_snooping [ vlan_name &lt;vlan_name 32&gt;  all] {host_timeout &lt;sec 1-16711450&gt;   router_timeout &lt;sec 1-16711450&gt;  leave_timer &lt;sec 1-16711450&gt;   state [enable disable]   fast_leave [enable disable]}(1)</b>
Description	This command allows the user to configure IGMP snooping on the Switch.
Parameters	<p><i>&lt;vlan_name 32&gt;</i> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p><i>host_timeout &lt;sec 1-16711450&gt;</i> – Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds.</p> <p><i>router_timeout &lt;sec 1-16711450&gt;</i> – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds.</p> <p><i>leave_timer &lt;sec 0-16711450&gt;</i> – Specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted. The default setting is 2.</p>

## config igmp\_snooping

Note: The leave timer does not need to be configured as its action has no effect on the IGMP snooping settings.

*state [enable | disable]* – Allows users to enable or disable IGMP snooping for the specified VLAN.

### Restrictions

Only Administrator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DES-1228/ME:4# config igmp_snooping default host_timeout 250 state enable
```

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

```
Success.
```

```
DES-1228/ME:4#
```

## config igmp\_snooping querier

### Purpose

Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping.

### Syntax

```
config igmp_snooping querier [ vlan_name <vlan_name 32> [all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable|disable] }(1)
```

### Description

The **config igmp\_snooping querier** command configures IGMP snooping querier.

### Parameters

*<vlan\_name 32>* – The name of the VLAN for which IGMP snooping querier is to be configured.

*query\_interval <sec 1-25>* – Specifies the amount of time in seconds between general query transmissions. the default setting is 125 seconds.

*max\_response\_time* – The maximum time in seconds to wait for reports from members. The default setting is 10 seconds.

*robustness\_variable* – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:

- Group member interval – Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
- Other querier present interval – Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
- Last member query count – Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.
- By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy.

*last\_member\_query\_interval* – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.

*state* – If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). If the state is disabled, then the switch can not play the role as a querier. Note that if the Layer 3 router connected to the switch provide only the IGMP

## config igmp\_snooping querier

proxy function but not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.

**Restrictions** Only Administrator-level users can issue this command.

Example usage:

To configure IGMP snooping querier:

```
DES-1228/ME:4# config igmp_snooping querier vlan default query_interval 125 state enable
Command: config igmp_snooping querier vlan default query_interval 125 state enable

Success.

DES-1228/ME:4#
```

## config router\_ports

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

Example usage:

To set up static router ports:

```
DES-1228/ME:4#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DES-1228/ME:4#
```

## config router\_ports\_forbidden

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

Example usage:

To set up forbidden router ports:

```
DES-1228/ME:4# config router_ports_forbidden default add 2-10
Command: config router_ports_forbidden default add 2-10

Success.

DES-1228/ME:4#
```

## enable igmp\_snooping

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

Example usage:

To enable IGMP snooping on the Switch:

```
DES-1228/ME:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DES-1228/ME:4#
```

## disable igmp\_snooping

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

Example usage:

To disable IGMP snooping on the Switch:

```
DES-1228/ME:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DES-1228/ME:4#
```

Example usage:

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

```
DES-1228/ME:4#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only

Success.

DES-1228/ME:4#
```

## show igmp\_snooping

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

Example usage:

To show IGMP snooping:

```

DES-1228/ME:4#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State           : Disabled
Multicast Router Only                 : Disabled
Data Driven Learning Max Entries      : 56

VLAN Name                             : default
Query Interval                         : 125
Max Response Time                      : 10
Robustness Value                       : 2
Last Member Query Interval            : 1
Host Timeout                           : 260
Route Timeout                           : 260
Leave Timer                              : 2
Querier State                          : Disabled
Querier Router Behavior                : Non-Querier
State                                  : Disabled
Multicast Fast Leave                  : Disabled
Data Driven Learning Aged Out         : Disabled

VLAN Name                             : RG
Query Interval                         : 125
Max Response Time                      : 10

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

```

## show router\_ports

Purpose	Used to display the currently configured router ports on the Switch.
Syntax	<b>show router_ports {vlan &lt;vlan_name 32&gt;} {[static   dynamic   forbidden]}</b>
Description	This command will display the router ports currently configured on the Switch.
Parameters	<p>&lt;vlan_name 32&gt; – The name of the VLAN on which the router port resides.</p> <p><i>static</i> – Displays router ports that have been statically configured.</p> <p><i>dynamic</i> – Displays router ports that have been dynamically configured.</p> <p><i>forbidden</i> – Displays forbidden router ports that have been statically configured.</p>
Restrictions	None.

Example usage:

To display the router ports.



```
DES-1228/ME:4#show router_ports
Command: show router_ports

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

Total Entries: 1

DES-1228/ME:4#
```

## show igmp\_snooping forwarding

Purpose	Used to display the current IGMP snooping forwarding state.
Syntax	<b>show igmp_snooping forwarding {vlan &lt;vlan_name 32&gt;}</b>
Description	Used to display the current IGMP snooping forwarding state.
Parameters	<vlan_name 32> – The name of the VLAN for which to view IGMP snooping group information.
Restrictions	None.

Example usage:

To view the current IGMP snooping forwarding:

```
DES-1228/ME:4#show igmp_snooping forwarding vlan default
Command: show igmp_snooping forwarding vlan default

Total Entries in VLAN default: 0

DES-1228/ME:4#
```

## show igmp\_snooping group

Purpose	Used to display the current IGMP snooping configuration on the Switch.
Syntax	<b>show igmp_snooping group {vlan &lt;vlan_name 32&gt;} {data_driven}</b>
Description	This command will display the current IGMP setup currently configured on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN for which to view IGMP snooping group information.  <i>data_driven</i> – hen the data driven learning is enabled, the multicast filtering mode for all ports are ignored.
Restrictions	None.

Example usage:

To view the current IGMP snooping group:

```
DES-1228/ME:4#show igmp_snooping group
```

```
Command: show igmp_snooping group
```

```
VLAN Name      : default
Multicast Group: 224.0.0.22
MAC Address     : 01-00-5E-00-00-16
Member Ports   :
Router Ports   : 1,13-20
```

```
VLAN Name      : default
Multicast Group: 239.255.255.250
MAC Address     : 01-00-5E-7F-FF-FA
Member Ports   :
Router Ports   : 1,13-20
```

```
Total Entries : 2
```

```
DES-1228/ME:4#
```

## config igmp snooping data\_driven\_learning

Purpose	Used to configure the data driven learning of a IGMP snooping group.
Syntax	<b>config igmp_snooping data_driven_learning [ vlan_name &lt;vlan_name 32&gt; [all] {aged_out [enable disable]}(1)</b>
Description	<p>This command is used to enable/disable the data driven learning of a IGMP snooping group.</p> <p>When data-driven learning is enabled for the VLAN, or when the switch receives the IP multicast traffic on this VLAN, an IGMP snooping group will be created. The learning of an entry is not activated by IGMP membership registration, but by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will acknowledge the aging out of the entry. For a data-driven entry, the entry can be specified so that it won't be ageout or that it will be ageout by the host_timeout timer.</p> <p>When the data driven learning is enabled, the multicast filtering mode for all ports are ignored so that the multicast packets will be forwarded to router ports.</p> <p>Note that if a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. The ageing out mechanism will follow the ordinary IGMP snooping entry.</p>
Parameters	<p>&lt;vlan_name 32&gt; – specifies the vlan name to be configured.</p> <p>all – specifies all data driven entries.</p> <p>aged_out – Used to enable/disable the aging on the entry. By default, the state is in disabled state.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the igmp snooping data driven entry:

```
DES-1228/ME:4#config igmp_snooping data_driven_learning vlan_name default aged_out
enable
Command: config igmp_snooping data_driven_learning vlan_name default aged_out enable

Success.

DES-1228/ME:4#
```

### config igmp\_snooping data\_driven\_learning max\_learned\_entry

Purpose	Used to configure the IGMP snooping data driven learning max learned entry.
Syntax	<b>config igmp_snooping data_driven_learning max_learned_entry &lt;value 1-64&gt;</b>
Description	Used to configure the IGMP snooping data driven learning max learned entry.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure igmp\_snooping data\_driven\_learning max\_learned\_entry:

```
DES-1228/ME:4# config igmp_snooping data_driven_learning max_learned_entry 1
Command: config igmp_snooping data_driven_learning max_learned_entry 1

Success.

DES-1228/ME:4#
```

### clear igmp snooping data\_driven\_group

Purpose	Used to delete the IGMP snooping group learned by data driven.
Syntax	<b>clear igmp_snooping data_driven_group [ vlan_name &lt;vlan_name 32&gt; [all   &lt;ipaddr&gt;]   all ]</b>
Description	Used to delete the IGMP snooping group learned by data driven. Note that this command is currently only for layer 2 switches.
Parameters	<i>all</i> – Delete all entries learned by data driven. <vlan_name 32> – Specifies the vlan name. <ipaddr> – Specifies the IP Address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete all the groups learned by data-driven :

```
DES-1228/ME:4# clear igmp snooping data_driven_group all
Command: clear igmp snooping data_driven_group all

Success.

DES-1228/ME:4#
```



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

Command	Parameters
config dhcp_relay	{ hops <value 1-16>   time <sec 0-65535>}(1)
config dhcp_relay add ipif System	<ipaddr>
config dhcp_relay delete ipif System	<ipaddr>
config dhcp_relay option_82 state	[enable   disable]
config dhcp_relay option_82 check	[enable   disable]
config dhcp_relay option_82 policy	[replace   drop   keep]
config dhcp_relay option_82 remote_id	[default   user_define <string 32> ]
show dhcp_relay	{ipif [System]}
enable dhcp_relay	
disable dhcp_relay	

Each command is listed in detail in the following sections.

### config dhcp\_relay

Purpose	Used to configure the DHCP/BOOTP relay feature of the switch.
Syntax	<b>config dhcp_relay { hops &lt;value 1-16&gt;   time &lt;sec 0-65535&gt;}(1)</b>
Description	This command is used to configure the DHCP/BOOTP relay feature.
Parameters	<i>hops &lt;value 1-16&gt;</i> – Specifies the maximum number of relay agent hops that the DHCP packets can cross. <i>time &lt;sec 0-65535&gt;</i> – If this time is exceeded; the Switch will not relay the DHCP packet.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config DHCP relay:

```
DES-1228/ME:4#config dhcp_relay hops 2 time 23
```

```
Command: config dhcp_relay hops 2 time 23
```

```
Success.
```

```
DES-1228/ME:4#
```

### config dhcp\_relay add ipif

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

Example usage:

To add an IP destination to the DHCP relay table:

```
DES-1228/ME:4#config dhcp_relay add ipif System 10.58.44.6
Command: config dhcp_relay add ipif System 10.58.44.6

Success.

DES-1228/ME:4#
```

## config dhcp\_relay delete ipif

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

Example usage:

To delete an IP destination from the DHCP relay table:

```
DES-1228/ME:4#config dhcp_relay delete ipif System 10.58.44.6
Command: config dhcp_relay delete ipif System 10.58.44.6

Success.

DES-1228/ME:4#
```

## config dhcp\_relay option\_82 state

Purpose	Used to configure the state of DHCP relay agent information option 82 of the switch.
Syntax	<b>config dhcp_relay option_82 state [enable   disable]</b>
Description	This command is used to configure the state of DHCP relay agent information option 82 of the switch.
Parameters	<i>enable</i> – When this field is toggled to <i>Enabled</i> 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.  <i>disable</i> – If the field is toggled to <i>disable</i> the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DES-1228/ME:4#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DES-1228/ME:4#
```

## config dhcp\_relay option\_82 check

Purpose	Used to configure the checking mechanism of DHCP relay agent information option 82 of the switch.
Syntax	<b>config dhcp_relay option_82 check [enable   disable]</b>
Description	This command is used to configure the checking mechanism of DHCP/BOOTP relay agent information option 82 of the switch.
Parameters	<p><i>enable</i> – When the field is toggled to <i>enable</i>, 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.</p> <p><i>disable</i> – When the field is toggled to <i>disable</i>, the relay agent will not check the validity of the packet's option 82 field.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 check:

```
DES-1228/ME:4#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DES-1228/ME:4#
```

## config dhcp\_relay option\_82 policy

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

Example usage:

To configure DHCP relay option 82 policy:

```
DES-1228/ME:4#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DES-1228/ME:4#
```



**config dhcp\_relay option\_82 remote id**

Purpose	Used to configure the processing of DHCP 82 remote id option for the DHCP.																		
Syntax	<b>config dhcp_relay option_82 remote_id [default   user_define &lt;string 32&gt;]</b>																		
Description	<p>Configures the processing of DHCP 82 option for the DHCP relay function.</p> <p>When DHCP 82 option is enabled, the DHCP packet received from the client will be inserted with option 82 field before being relayed to the server. The DHCP 82 option contained 2 suboptions which is circuit ID suboption and remote ID suboption.</p> <p>The formats for the circuit ID suboption and the remote ID suboption are as following. For the circuit ID suboption of a standalone switch, the module field is always zero.</p> <p>Remote ID suboption format 2 (Using user-defined string as remote ID):</p> <table border="1" style="margin-left: 40px;"> <tr> <td style="text-align: center;">1.</td> <td style="text-align: center;">2.</td> <td style="text-align: center;">3.</td> <td style="text-align: center;">4.</td> <td style="text-align: center;">5.</td> <td></td> </tr> <tr> <td style="text-align: center;">2</td> <td style="text-align: center;">n + 2</td> <td style="text-align: center;">1</td> <td style="text-align: center;">n</td> <td colspan="2" style="text-align: center;">User-defined string</td> </tr> <tr> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td colspan="2" style="text-align: center;">6 bytes</td> </tr> </table> <p>1. Suboption type 2. Length : the string length of Remote ID suboption  3. Remote ID type 4. Length : the string length of user-defined string  5. User-defined string</p>	1.	2.	3.	4.	5.		2	n + 2	1	n	User-defined string		1 byte	1 byte	1 byte	1 byte	6 bytes	
1.	2.	3.	4.	5.															
2	n + 2	1	n	User-defined string															
1 byte	1 byte	1 byte	1 byte	6 bytes															
Parameters	None.																		
Restrictions	Only Administrator-level users can issue this command.																		

Example usage:

To configure DHCP relay option 82 remote id :

```
DES-1228/ME:4#config dhcp_relay option_82 remote_id user_define "D-Link L2 Switch"
Command: config dhcp_relay option_82 remote_id user_define "D-Link L2 Switch"

DES-1228/ME:4#
```

## show dhcp\_relay

Purpose	Used to display the current DHCP/BOOTP relay configuration.
Syntax	<b>show dhcp_relay {ipif [System]}</b>
Description	This command will display the current DHCP relay configuration for the Switch.
Parameters	<i>ipif System</i> – The name of the IP interface for which to display the current DHCP relay configuration.
Restrictions	None.

Example usage:

To show the DHCP relay configuration:

```
DES-1228/ME:4#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status      : Disabled
DHCP/BOOTP Hops Count Limit  : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State      : Disabled
DHCP Relay Agent Information Option 82 Check     : Disabled
DHCP Relay Agent Information Option 82 Policy    : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-19-5B-EF-78-B5

Interface      Server 1      Server 2      Server 3      Server 4
-----
DES-1228/ME:4#
```

Example usage:

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

```
DES-1228/ME:4#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

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

DES-1228/ME:4#
```

## enable dhcp\_relay

Purpose	Used to enable the DHCP/BOOTP relay function on the Switch.
Syntax	<b>enable dhcp_relay</b>
Description	This command is used to enable the DHCP/BOOTP relay function on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable DHCP relay:

```
DES-1228/ME:4#enable dhcp_relay
Command: enable dhcp_relay

Success.

DES-1228/ME:4#
```

## disable dhcp\_relay

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

Example usage:

To disable DHCP relay:

```
DES-1228/ME:4#disable dhcp_relay
Command: disable dhcp_relay

Success.

DES-1228/ME:4#
```

## 802.1X COMMANDS

The DES-1228/ME implements IEEE 802.1X Port-based and Host-based Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames.

Command	Parameters
enable 802.1x	
disable 802.1x	
show 802.1x auth_state	{ports <auth_portlist>}
show 802.1x auth_configuration	{ports <auth_portlist>}
config 802.1x capability ports	[<auth_portlist>   all] [authenticator   none]
config 802.1x auth_parameter ports	[ <portlist>  all] [default   {direction [both in]   port_control [force_unauth auto force_auth]   quiet_period <sec 0-65535>   tx_period <sec 1-65535>   supp_timeout <sec 1-65535>   server_timeout <sec 1-65535>   max_req <value 1-10>   reauth_period <sec 1-65535>   enable_reauth [enable disable]}(1)]
config 802.1x auth_protocol	[radius_eap   local]
config 802.1x init	{port_based ports [<auth_portlist>   all]   mac_based [ports] [<auth_portlist>  all] {mac_address <macaddr>}}
config 802.1x auth_mode	[port_based   mac_based]
config 802.1x reauth	{port_based ports [<portlist>   all]   mac_based [ports] [<portlist>   all] {mac_address <macaddr>}}
config radius add	<server_index 1-3> <server_ip> key <passwd 32> [ default   { auth_port<udp_port_number 1-65535>   acct_port <udp_port_number 1-65535>}(1)]
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> {ipaddress <server_ip>  key <passwd 32>   auth_port <udp_port_number 1-65535>   acct_port <udp_port_number 1-65535>}(1)
config radius parameter	{timeout <int 1-255>   retransmit <int 1-255>}(1)
show radius	
create 802.1x guest_vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist>   all] state [enable   disable]
delete 802.1x guest_vlan	{<vlan_name 32>}
show 802.1x guest_vlan	
show auth_statistics	{ports <auth_portlist>}
show auth_diagnostics	{ports <auth_portlist>}
show auth_session_statistics	{ports <auth_portlist>}
show auth_client	
show acct_client	
create 802.1x user	<username 15>
delete 802.1x user	<username 15>

Command	Parameters
show 802.1x user	

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

## enable 802.1x

Purpose	Used to enable the 802.1X server on the Switch.
Syntax	<b>enable 802.1x</b>
Description	The <b>enable 802.1x</b> command enables the 802.1X Network Access control application on the Switch. To select between port-based or Host-based, use the <b>config 802.1x auth_mode</b> command.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable 802.1X switch wide:

```
DES-1228/ME:4#enable 802.1x
Command: enable 802.1x

Success.

DES-1228/ME:4#
```

## disable 802.1x

Purpose	Used to disable the 802.1X server on the Switch.
Syntax	<b>disable 802.1x</b>
Description	The <b>disable 802.1x</b> command is used to disable the 802.1X Network Access control application on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable 802.1x on the Switch:

```
DES-1228/ME:4#disable 802.1x
Command: disable 802.1x

Success.

DES-1228/ME:4#
```

**show 802.1x auth\_configuration**

Purpose	Used to display the current configuration of the 802.1X server on the Switch.
Syntax	<b>show 802.1x auth_configuration {ports &lt;auth_portlist&gt;}</b>
Description	The <b>show 802.1x auth_configuration</b> command is used to display the 802.1X Port-based or Host-based Network Access control local users currently configured on the Switch.
Parameters	<p><i>ports &lt;auth_portlist&gt;</i> – Specifies a port or range of ports to view.</p> <p>The following details are displayed:</p> <p><i>802.1x Enabled / Disabled</i> – Shows the current status of 802.1X functions on the Switch.</p> <p><i>Authentication Mode</i> – Shows the authentication mode, whether it be by MAC address or by port.</p> <p><i>Authentication Protocol</i> – Shows the authentication protocol suite in use between the Switch and a RADIUS server. May read <i>Radius_Eap</i> or <i>local</i>.</p> <p><i>Port number</i> – Shows the physical port number on the Switch.</p> <p>Capability: <i>Authenticator/None</i> – Shows the capability of 802.1X functions on the port number displayed above. There are two 802.1X capabilities that can be set on the Switch: Authenticator and None.</p> <p><i>AdminCtlDir: Both / In</i> – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.</p> <p><i>OpenCtlDir: Both / In</i> – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.</p> <p><i>Port Control: ForceAuth / ForceUnauth / Auto</i> – 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.</p> <p><i>QuietPeriod</i> – This is the initialization value of the quiet period timer. The default value is 60s and can be any value between 0-65535.</p> <p><i>TxPeriod</i> – This is the initialization value of the tx timer. The default value is 30s and can be any value between 1-65535.</p> <p><i>SuppTimeout</i> – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request / Identity packets.</p> <p><i>ServerTimeout</i> – Shows the length of time to wait for a response from a RADIUS server.</p> <p><i>MaxReq</i> – Shows the maximum number of times to retry sending packets to the supplicant.</p> <p><i>ReAuthPeriod</i> – Shows the time interval between successive re-authentications.</p> <p><i>ReAuthenticate: Enabled / Disabled</i> – Shows whether or not to re-authenticate.</p>
Restrictions	None.

Example usage:

To display the 802.1X authentication states:

```
DES-1228/ME:4#show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X                : Enabled
Authentication Mode   : Port_based
Authentication Protocol : Radius_EAP
```

```

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

```

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

## show 802.1x auth\_state

Purpose	Used to display the current authentication state of the 802.1X server on the Switch.
Syntax	<b>show 802.1x auth_state {ports &lt;auth_portlist&gt;}</b>
Description	The <b>show 802.1x auth_state</b> command is used to display the current authentication state of the 802.1X Port-based or Host-based Network Access Control application on the Switch.
Parameters	<p>&lt;auth_portlist&gt; – Specifies a port or range of ports to be viewed.</p> <p>The following details what is displayed:</p> <p>Port number – Shows the physical port number on the Switch.</p> <p>Auth PAE State: Initalize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE.</p> <p>Backend State: Request / Response / Fail / Idle / Initalize / Success / Timeout – Shows the current state of the Backend Authenticator.</p> <p>Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.</p>
Restrictions	None.

Example usage:

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

```
DES-1228/ME:4#show 802.1x auth_state
```

```
Command: show 802.1x auth_state
```

Port	Auth PAE State	Backend State	Port Status
-----	-----	-----	-----
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized

```

4          ForceAuth      Success      Authorized
5          ForceAuth      Success      Authorized
6          ForceAuth      Success      Authorized
7          ForceAuth      Success      Authorized
8          ForceAuth      Success      Authorized
9          ForceAuth      Success      Authorized
10         ForceAuth      Success      Authorized
11         ForceAuth      Success      Authorized
12         ForceAuth      Success      Authorized
13         ForceAuth      Success      Authorized
14         ForceAuth      Success      Authorized
15         ForceAuth      Success      Authorized
16         ForceAuth      Success      Authorized
17         ForceAuth      Success      Authorized
18         ForceAuth      Success      Authorized
19         ForceAuth      Success      Authorized
20         ForceAuth      Success      Authorized

```

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

Example usage:

To display the 802.1X auth state for Host-based 802.1X:

```
DES-1228/ME:4#show 802.1x auth_state
```

```
Command: show 802.1x auth_state
```

Port	Auth PAE State	Backend State	Port Status
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized

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

## config 802.1x auth\_mode



## config 802.1x auth\_mode

Purpose	Used to configure the 802.1X authentication mode on the Switch.
Syntax	<b>config 802.1x auth_mode {port_based   mac_based}</b>
Description	The <b>config 802.1x auth_mode</b> command is used to enable either the port-based or Host-based 802.1X authentication feature on the Switch.
Parameters	<i>[port_based   mac_based]</i> – The Switch allows users to authenticate 802.1X by either port or MAC address.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure 802.1X authentication by MAC address:

```
DES-1228/ME:4#config 802.1x auth_mode mac_based
```

```
Command: config 802.1x auth_mode mac_based
```

Success.

```
DES-1228/ME:4#
```

## config 802.1x capability ports

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

Example usage:

To configure 802.1X capability on ports 1-10:

```
DES-1228/ME:4#config 802.1x capability ports 1-10 authenticator
```

```
Command: config 802.1x capability ports 1-10 authenticator
```

Success.

```
DES-1228/ME:4#
```

## config 802.1x auth\_parameter

Purpose	Used to configure the 802.1X Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1X settings.
Syntax	<b>config 802.1x auth_parameter ports [ &lt;portlist&gt;  all] [default   {direction [both in]   port_control [force_unauth auto force_auth]   quiet_period &lt;sec 0-65535&gt;   tx_period &lt;sec 1-65535&gt;   supp_timeout &lt;sec 1-65535&gt;   server_timeout &lt;sec 1-65535&gt;   max_req &lt;value 1-10&gt;   reauth_period &lt;sec 1-65535&gt;   enable_reauth [enable disable]}(1)]</b>
Description	The <b>config 802.1x auth_parameter</b> command is used to configure the 802.1X Authentication parameters on a range of ports. The default parameter will return all ports

**config 802.1x auth\_parameter**

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

Example usage:

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

```
DES-1228/ME:4#config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

DES-1228/ME:4#
```

## config 802.1x auth\_protocol

Purpose	Used to configure the 802.1X authentication protocol on the Switch.
Syntax	<b>config 802.1x auth_protocol [local   radius_eap]</b>
Description	The <b>config 802.1x auth_protocol</b> command enables users to configure the authentication protocol.
Parameters	<i>radius_eap</i>   <i>local</i> – Specify the type of authentication protocol desired.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the authentication protocol on the Switch:

```
DES-1228/ME:4# config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DES-1228/ME:4#
```

## config 802.1x init

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

Example usage:

To initialize the authentication state machine of all ports:

```
DES-1228/ME:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-1228/ME:4#
```

## config 802.1x reauth

Purpose	Used to configure the 802.1X re-authentication feature of the Switch.
Syntax	<b>config 802.1x reauth {port_based ports [&lt;auth_portlist&gt;   all]   mac_based   ports [&lt;portlist&gt;   all] {mac_address &lt;macaddr&gt;}}</b>
Description	The <b>config 802.1x reauth</b> command is used to re-authenticate a previously authenticated device based on port number.
Parameters	<p><i>port_based</i> – This instructs the Switch to re-authorize 802.1X functions based only on the port number. Ports approved for re-authorization can then be specified.</p> <p><i>mac_based</i> – This instructs the Switch to re-authorize 802.1X functions based only on the port number or the MAC address. MAC addresses approved for re-authorization can then be specified.</p> <p><i>ports &lt;auth_portlist&gt;</i> – Specifies a port or range of ports to be re-authorized.</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>mac_address &lt;macaddr&gt;</i> – Enter the MAC address to be re-authorized.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure 802.1X reauthentication for ports 1-18:

```
DES-1228/ME:4#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-1228/ME:4#
```

## config radius add

Purpose	Used to configure the settings the Switch will use to communicate with a RADIUS server.
Syntax	<b>config radius add &lt;server_index 1-3&gt; &lt;server_ip&gt; key &lt;passwd 32&gt; [ default   { auth_port&lt;udp_port_number 1-65535&gt;   acct_port &lt;udp_port_number 1-65535&gt;}(1)]</b>
Description	The <b>config radius add</b> command is used to configure the settings the Switch will use to communicate with a RADIUS server.
Parameters	<p><i>&lt;server_index 1-3&gt;</i> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the Switch.</p> <p><i>&lt;server_ip&gt;</i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.</p> <p><i>&lt;passwd 32&gt;</i> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used.</p> <p><i>default</i> – Uses the default UDP port number in both the “auth_port” and “acct_port” settings.</p>

## config radius add

*auth\_port* <udp\_port\_number 1-65535> – The UDP port number for authentication requests. The default is 1812.

*acct\_port* <udp\_port\_number 1-65535> – The UDP port number for accounting requests. The default is 1813.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DES-1228/ME:4#config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default
```

Success.

```
DES-1228/ME:4#
```

## config radius delete

Purpose Used to delete a previously entered RADIUS server configuration.

Syntax **config radius delete <server\_index 1-3>**

Description The **config radius delete** command is used to delete a previously entered RADIUS server configuration.

Parameters <server\_index 1-3> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the Switch.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DES-1228/ME:4#config radius delete 1
Command: config radius delete 1
```

Success.

```
DES-1228/ME:4#
```

## config radius

Purpose Used to configure the Switch's RADIUS settings.

Syntax **config radius <server\_index 1-3> {ipaddress <server\_ip> | key <passwd 32> | auth\_port <udp\_port\_number 1-65535> | acct\_port <udp\_port\_number 1-65535>}(1)**

Description The **config radius** command is used to configure the Switch's RADIUS settings.

Parameters <server\_index 1-3> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the Switch.

*ipaddress* <server\_ip> – The IP address of the RADIUS server.

*key* – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.

- <passwd 32> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used.

*auth\_port* <udp\_port\_number 1-65535> – The UDP port number for authentication

## config radius

requests. The default is 1812.

*acct\_port* <udp\_port\_number 1-65535> – The UDP port number for accounting requests. The default is 1813.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DES-1228/ME:4#config radius 1 10.48.74.121 key dlink default
Command: config radius 1 10.48.74.121 key dlink default
```

Success.

```
DES-1228/ME:4#
```

## config radius parameter

Purpose Used to configure parameters for radius servers.

Syntax **config radius parameter {timeout <int 1-255> | retransmit <int 1-255>}(1)**

Description Used to configure parameters for radius servers.

Parameters *timeout* <int 1-255> – The time in second for waiting server reply. Default value is 5 seconds.  
*retransmit* <int 1-255> – The count for re-transmit. Default value is 2.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the timeout option for radius servers.

```
DES-1228/ME:4# config radius parameter timeout 3
Command: config radius parameter timeout 3
```

Success.

```
DES-1228/ME:4#
```

## show radius

Purpose Used to display the current RADIUS configurations on the Switch.

Syntax **show radius**

Description The **show radius** command is used to display the current RADIUS configurations on the Switch.

Parameters None.

Restrictions None.

Example usage:

To display RADIUS settings on the Switch:

```
DES-1228/ME:4#show radius
Command: show radius
```

```
Timeout      : 5 seconds
Retransmit   : 2
```

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

```
Total Entries : 3
```

```
DES-1228/ME:4#
```

## create 802.1x guest\_vlan

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

Example usage:

To configure a previously created VLAN as an 802.1X Guest VLAN for the Switch:

```
DES-1228/ME:4#create 802.1x guest_vlan Trinity
Command: create 802.1x guest_vlan Trinity

Success.

DES-1228/ME:4#
```

## config 802.1x guest\_vlan ports

Purpose	Used to configure ports for a pre-existing 802.1X guest VLAN.
Syntax	<b>config 802.1x guest_vlan ports [&lt;portlist&gt;   all] state [enable   disable]</b>
Description	The <b>config 802.1x guest_vlan ports</b> command is used to configure ports to be enabled or disabled for the 802.1X guest VLAN.
Parameters	<b>&lt;portlist&gt;</b> – Specify a port or range of ports to be configured for the 802.1X Guest VLAN. <b>all</b> – Specify this parameter to configure all ports for the 802.1X Guest VLAN. <b>state [enable   disable]</b> – Use these parameters to enable or disable port listed here as enabled or disabled for the 802.1X Guest VLAN.
Restrictions	Only Administrator-level users can issue this command. Users must have already previously created a VLAN using the <b>create vlan</b> command. If

## config 802.1x guest\_vlan ports

the specific port state changes from an enabled state to a disabled state, these ports will return to the default VLAN.

Example usage:

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

```
DES-1228/ME:4#config 802.1x guest_vlan ports 1-5 state enable
```

```
Command: config 802.1x guest_vlan ports 1-5 state enable
```

```
Success.
```

```
DES-1228/ME:4#
```

## show 802.1x guest\_vlan

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

Example usage:

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

```
DES-1228/ME:4#show 802.1x guest_vlan
```

```
Command: show 802.1x guest_vlan
```

```
Guest VLAN Setting
```

```
-----
```

```
Guest VLAN : Trinity
```

```
Enable guest VLAN ports: 1-5
```

```
DES-1228/ME:4#
```

## delete 802.1x guest\_vlan

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



Example usage:

To delete a previously created 802.1X Guest VLAN.

```
DES-1228/ME:4#delete 802.1x guest_vlan Trinity
Command: delete 802.1x guest_vlan Trinity

Success.

DES-1228/ME:4#
```

## show acct\_client

Purpose	Used to display the current RADIUS accounting client.
Syntax	<b>show acct_client</b>
Description	The <b>show acct_client</b> command is used to display the current RADIUS accounting client currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS accounting client:

```
DES-1228/ME:4#show acct_client
Command: show acct_client

radiusAcctClient
-----
radiusAcctClientInvalidServerAddresses      0
radiusAcctClientIdentifier                  D-Link

radiusAuthServerEntry                       0
-----
radiusAccServerIndex                        1
radiusAccServerAddress                      10.53.13.199
radiusAccClientServerPortNumber             0
radiusAccClientRoundTripTime                0
radiusAccClientRequests                     0
radiusAccClientRetransmissions              0
radiusAccClientResponses                    0
radiusAccClientMalformedResponses           0
radiusAccClientBadAuthenticators            0
radiusAccClientPendingRequests              0
radiusAccClientTimeouts                     0
radiusAccClientUnknownTypes                 0
radiusAccClientPacketsDropped               0
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

## show auth\_client

Purpose	Used to display the current RADIUS authentication client.
Syntax	<b>show auth_client</b>

## show auth\_client

Description	The <b>show auth_client</b> command is used to display the current RADIUS authentication client currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS authentication client:

```
DES-1228/ME:4#show auth_client
Command: show auth_client

radiusAuthClient
-----
radiusAuthClientInvalidServerAddresses      0
radiusAuthClientIdentifier                  D-Link

radiusAuthServerEntry                       0
-----
radiusAuthServerIndex                       : 1
radiusAuthServerAddress                     : 0.0.0.0
radiusAuthClientServerPortNumber           0
radiusAuthClientRoundTripTime              0
radiusAuthClientAccessRequests             0
radiusAuthClientAccessRetransmissions      0
radiusAuthClientAccessAccepts              0
radiusAuthClientAccessRejects              0
radiusAuthClientAccessChallenges           0
radiusAuthClientMalformedAccessResponses   0
radiusAuthClientBadAuthenticators          0
radiusAuthClientPendingRequests            0
radiusAuthClientTimeouts                   0
radiusAuthClientUnknownTypes               0
radiusAuthClientPacketsDropped             0
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

## show auth\_diagnostics

Purpose	Used to display the current authentication diagnostics.
Syntax	<b>show auth_diagnostics {ports [&lt;auth_portlist&gt;]}</b>
Description	The <b>show auth_diagnostics</b> command is used to display the current authentication diagnostics of the Switch on a per port basis.
Parameters	<i>ports &lt;auth_portlist&gt;</i> – Specifies a range of ports.
Restrictions	None.

Example usage:

To display the current authentication diagnostics for port 1 of module 1:

```

DES-1228/ME:4#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port number : 1

EntersConnecting                0
EapLogoffsWhileConnecting      0
EntersAuthenticating           0
SuccessWhileAuthenticating     0
TimeoutsWhileAuthenticating    0
FailWhileAuthenticating        0
ReauthsWhileAuthenticating     0
EapStartsWhileAuthenticating   0
EapLogoffWhileAuthenticating   0
ReauthsWhileAuthenticated     0
EapStartsWhileAuthenticated    0
EapLogoffWhileAuthenticated    0
BackendResponses                0
BackendAccessChallenges        0
BackendOtherRequestsToSupplicant 0
BackendNonNakResponsesFromSupplicant 0
BackendAuthSuccesses           0
BackendAuthFails               0

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

```

## show auth\_session\_statistics

Purpose	Used to display the current authentication session statistics.
Syntax	<b>show auth_session_statistics {ports &lt;auth_portlist   all&gt;}</b>
Description	The <b>show auth_session</b> statistics command is used to display the current authentication session statistics of the Switch on a per port basis.
Parameters	<i>ports &lt;auth_portlist&gt;</i> – Specifies a range of ports. <i>all</i> – Specifies that all ports will be viewed.
Restrictions	None.

Example usage:

To display the current authentication session statistics for port 16 of module 1:

```
DES-1228/ME:4#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port number : 1

SessionOctetsRx           0
SessionOctetsTx           0
SessionFramesRx           0
SessionFramesTx           0
SessionId
SessionAuthenticMethod    Remote Authentication Server
SessionTime                0
SessionTerminateCause     SupplicantLogoff
SessionUserName            Trinity

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

## show auth\_statistics

Purpose	Used to display the current authentication statistics.
Syntax	<b>show auth_statistics {ports &lt;auth_portlist&gt;}</b>
Description	The <b>show auth_statistics</b> command is used to display the current authentication statistics of the Switch on a per port basis.
Parameters	<i>ports &lt;auth_portlist&gt;</i> – Specifies a range of ports.
Restrictions	None.

Example usage:

To display the current authentication statistics for port 1:16:

```
DES-1228/ME:4#show auth_statistics ports 1
Command: show auth_statistics ports 1

Port number : 1

EapolFramesRx           0
EapolFramesTx           0
EapolStartFramesRx      0
EapolReqIdFramesTx      0
EapolLogoffFramesRx     0
EapolReqFramesTx        0
EapolRespIdFramesRx     0
EapolRespFramesRx       0
InvalidEapolFramesRx    0
EapolLengthErrorFramesRx 0

LastEapolFrameVersion    0
LastEapolFrameSource     00-00-00-00-00-00

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

## create 802.1x user

Purpose	Used to create a new 802.1X user.
Syntax	<b>create 802.1x user &lt;username 15&gt;</b>
Description	The <b>create 802.1x user</b> command is used to create new 802.1X users.
Parameters	<username 15> – A username of up to 15 alphanumeric characters in length.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an 802.1X user:

```
DES-1228/ME:4#create 802.1x user dtremblett
Command: create 802.1x user dtremblett

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

DES-1228/ME:4#
```

## show 802.1x user

Purpose	Used to display the 802.1X user accounts on the Switch.
Syntax	<b>show 802.1x user</b>
Description	The <b>show 802.1x user</b> command is used to display the 802.1X Port-based or Host-based Network Access control local users currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view 802.1X users currently configured on the Switch:

```
DES-1228/ME:4#show 802.1x user
Command: show 802.1x user

Index                UserName
-----                -
Darren                Trinity

Total Entries: 1

DES-1228/ME:4#
```

## delete 802.1x user

Purpose	Used to delete an 802.1X user account on the Switch.
Syntax	<b>delete 802.1x user &lt;username 15&gt;</b>
Description	The <b>delete 802.1x user</b> command is used to delete the 802.1X Port-based or Host-based Network Access control local users currently configured on the Switch.
Parameters	<username 15> – A username can be as many as 15 alphanumeric characters.

## delete 802.1x user

Restrictions Only Administrator-level users can issue this command.

Example usage:

To delete 802.1X users:

```
DES-1228/ME:4#delete 802.1x user dtremblett
```

```
Command: delete 802.1x user dtremblett
```

```
Are you sure to delete the user?(y/n)
```

```
Success.
```

```
DES-1228/ME:4#
```

## ACCESS CONTROL LIST (ACL) COMMANDS

The DES-1228/ME implements Access Control Lists that enable the Switch to deny network access to specific devices or device groups based on IP settings and MAC address.

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

Command	Parameters
create access_profile	[ ethernet { vlan   source_mac <macmask>   destination_mac <macmask>   802.1p   ethernet_type }(1)   ip { vlan   source_ip_mask <netmask>   destination_ip_mask <netmask>   dscp   [ icmp   igmp   tcp {src_port_mask <hex 0x0-0xffff>   dst_port_mask <hex 0x0-0xffff>   flag_mask [ all   {urg   ack   psh   rst   syn   fin}(1)] }   udp {src_port_mask <hex 0x0-0xffff>   dst_port_mask <hex 0x0-0xffff> }   protocol_id_mask <hex 0x0-0xff>}}(1)] profile_id <value 1-256>
delete access_profile	[profile_id <value 1-256>   all]
config access_profile	profile_id <value 1-256> [ add access_id [ auto_assign   <value 1-65535> ] [ ethernet { vlan <vlan_name 32>   source_mac <macaddr>   destination_mac <macaddr>   802.1p <value 0-7>   ethernet_type <hex 0x0-0xffff> }(1)   ip { vlan <vlan_name 32>   source_ip <ipaddr>   destination_ip <ipaddr>   dscp <value 0-63>   [ icmp   igmp   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> }](1)] port [<portlist>   all ] [ permit{ priority <value 0-7>   replace_priority_with <value 0-7>   rx_rate [ no_limit  <value 64-1024000>]} deny mirror ]   delete access_id <value 1-65535> ]
show access_profile	profile_id <value 1-256>
enable cpu_interface_filtering	
disable cpu_interface_filtering	
create cpu access_profile profile_id	<value 1-3> [ ethernet { vlan   source_mac <macmask>   destination_mac <macmask>   802.1p   ethernet_type } (1)   ip { vlan   source_ip_mask <netmask>   destination_ip_mask <netmask>   dscp   [ icmp { type   code }   igmp { type }   tcp {src_port_mask <hex 0x0-0xffff>   dst_port_mask <hex 0x0-0xffff>   flag_mask [ all   {urg   ack   psh   rst   syn   fin}(1)] }   udp {src_port_mask <hex 0x0-0xffff>   dst_port_mask <hex 0x0-0xffff> }   protocol_id_mask <hex 0x0-0xff> {user_define <hex 0x0-0xffffffff>}}(1)]
delete cpu access_profile	profile_id <value 1-3>
config cpu access_profile profile_id	<value 1-3> [ add access_id <value 1-5> [ ethernet { vlan <vlan_name 32>   source_mac <macaddr>   destination_mac <macaddr>   802.1p <value 0-7>   ethernet_type <hex 0x0-0xffff> }(1)   ip { vlan <vlan_name 32>   source_ip <ipaddr>   destination_ip <ipaddr>   dscp <value 0-63>   [ icmp {type <value 0-255>   code <value 0-255>}   igmp {type <value 0-255>}   tcp {src_port <value 0-65535>   dst_port <value 0-65535>   urg   ack   psh   rst   syn   fin }   udp {src_port <value 0-65535>   dst_port <value 0-65535> }   protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}}(1)] port [<portlist>   all ] [ permit   deny ]   delete access_id <value 1-5> ]
show cpu access_profile	profile_id <value 1-3>

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

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

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

**create access\_profile ip source\_ip\_mask 255.255.255.0 profile\_id 1 profile\_name 1**

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

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

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

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

**config access\_profile profile\_id 1 add access\_id 1 ip source\_ip 10.42.73.1 port 7 deny**

We use the **profile\_id 1** which was specified when the access profile was created. The **add** parameter instructs the Switch to add the criteria that follows to the list of rules that are associated with access profile 1. For each rule entered into the access profile, users can assign an **access\_id** that identifies the rule within the list of rules. The **access\_id** is an index number only and does not effect priority within the **profile\_id**. This **access\_id** may be used later if users want to remove the individual rule from the profile.

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

**create access\_profile**

Purpose	Used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the <b>config access_profile</b> command, below.
Syntax	<b>create access_profile [ ethernet { vlan   source_mac &lt;macmask&gt;   destination_mac &lt;macmask&gt;   802.1p   ethernet_type }(1)   ip { vlan   source_ip_mask &lt;netmask&gt;   destination_ip_mask &lt;netmask&gt;   dscp   [ icmp   igmp   tcp {src_port_mask &lt;hex 0x0-0xffff&gt;   dst_port_mask &lt;hex 0x0-0xffff&gt;   flag_mask [ all   {urg   ack   psh   rst   syn   fin}(1)]}   udp {src_port_mask &lt;hex 0x0-0xffff&gt;   dst_port_mask &lt;hex 0x0-0xffff&gt;}   protocol_id_mask &lt;hex 0x0-0xff&gt;}] (1) profile_id &lt;value 1-256&gt;</b>
Description	The <b>create access_profile</b> command is used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the <b>config access_profile</b> command, below.
Parameters	<p><b>ethernet</b> – Specifies that the Switch will examine the layer 2 part of each packet header.</p> <p><b>vlan</b> – Specifies that the Switch will examine the VLAN part of each packet header.</p> <p><b>source_mac &lt;macmask&gt;</b> – Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format.</p> <p><b>destination_mac &lt;macmask&gt;</b> – Specifies a MAC address mask for the destination MAC address.</p> <p><b>802.1p</b> – Specifies that the Switch will examine the 802.1p priority value in the frame's header.</p> <p><b>ethernet_type</b> – Specifies that the Switch will examine the Ethernet type value in each frame's header.</p>



**create access\_profile**

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

*vlan* – Specifies a VLAN mask.

*source\_ip\_mask* <netmask> – Specifies an IP address mask for the source IP address.

*destination\_ip\_mask* <netmask> – Specifies an IP address mask for the destination IP address.

*dscp* – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.

*icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.

*igmp* – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.

*src\_port\_mask* <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.

*dst\_port\_mask* <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.

*flag\_mask* – Enter the appropriate flag\_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between *all*, *urg* (urgent), *ack* (acknowledgement), *psh* (push), *rst* (reset), *syn* (synchronize) and *fin* (finish).

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

*src\_port\_mask* <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.

*dst\_port\_mask* <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.

*protocol\_id\_mask* – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.

*profile\_id* <value 1-256> – Sets the relative priority for the profile. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 to 256.

**Restrictions** Only Administrator-level users can issue this command.

Example usage:

To create an access list rules:

```
DES-1228/ME:4#create access_profile ip vlan source_ip_mask 20.0.0.0 destination_ip_mask
10.0.0.0 dscp icmp profile_id 101
Command: create access_profile ip vlan source_ip_mask 20.0.0.0 destination_ip_mask
10.0.0.0 dscp icmp permit profile_id 101
```

Success.

```
DES-1228/ME:4#
```

## delete access\_profile

Purpose	Used to delete a previously created access profile.
Syntax	<b>delete access_profile</b> [ <b>profile_id</b> <value 1-256>   <b>all</b> ]
Description	The <b>delete access_profile</b> command is used to delete a previously created access profile on the Switch.
Parameters	<i>profile_id</i> <value 1-256> – Enter an integer between 1 and 256 that is used to identify the access profile that will be deleted with this command. This value is assigned to the access profile when it is created with the <b>create access_profile</b> command. The user may enter a profile ID number between 1 and 256. <i>all</i> – Specifies all access list profiles will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4# delete access_profile profile_id 1
```

```
Command: delete access_profile profile_id 1
```

```
Success.
```

```
DES-1228/ME:4#
```

## config access\_profile

Purpose	Used to configure an access profile on the Switch and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the <b>create access_profile</b> command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the <b>config access_profile</b> command, below.
Syntax	<b>config access_profile</b> <i>profile_id</i> <value 1-256> [ <b>add access_id</b> [ <i>auto_assign</i>   <value 1-65535> ] [ <b>ethernet</b> { <i>vlan</i> <vlan_name 32>   <b>source_mac</b> <macaddr>   <b>destination_mac</b> <macaddr>   <b>802.1p</b> <value 0-7>   <b>ethernet_type</b> <hex 0x0-0xffff> }(1)   <b>ip</b> { <i>vlan</i> <vlan_name 32>   <b>source_ip</b> <ipaddr>   <b>destination_ip</b> <ipaddr>   <b>dscp</b> <value 0-63>   [ <b>icmp</b>   <b>igmp</b>   <b>tcp</b> { <i>src_port</i> <value 0-65535>   <b>dst_port</b> <value 0-65535>   <b>urg</b>   <b>ack</b>   <b>psh</b>   <b>rst</b>   <b>syn</b>   <b>fin</b> }   <b>udp</b> { <i>src_port</i> <value 0-65535>   <b>dst_port</b> <value 0-65535> }   <b>protocol_id</b> <value 0 - 255> }](1) ] <b>port</b> [ <portlist>   <b>all</b> ] [ <b>permit</b> { <i>priority</i> <value 0-7>   <b>replace_priority_with</b> <value 0-7>   <b>rx_rate</b> [ <b>no_limit</b>   <value 64-1024000>]}   <b>deny</b>   <b>mirror</b> ]   <b>delete access_id</b> <value 1-65535> ]
Description	The <b>config access_profile</b> command is used to configure an access profile on the Switch and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the <b>create access_profile</b> command, above.
Parameters	<i>profile_id</i> <value 1-256> – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the <b>create access_profile</b> command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 and 256. <i>add access_id</i> <value 1-65535> – Adds an additional rule to the above specified access profile. The value is used to index the rule created. For information on number of rules that can be created for a given port, please see the introduction to this chapter.

**config access\_profile**

*auto\_assign* – Choose this parameter to configure the Switch to automatically assign a numerical value (between 1 and 65535) for the rule being configured.

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

*vlan* <vlan\_name 32> – Specifies that the access profile will apply to only to this VLAN.

*source\_mac* <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address.

*destination\_mac* <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address.

*802.1p* <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.

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

**Parameters**

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

*vlan* <vlan\_name 32> – Specifies that the access profile will apply to only this VLAN.

*source\_ip* <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address.

*destination\_id* <value 0-255> – Specifies that the access profile will apply to only packets with this destination IP address.

*dscp* <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header

*icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.

*igmp* – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

*tcp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.

*src\_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.

*dst\_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.

*urg*: TCP control flag (urgent)

*ack*: TCP control flag (acknowledgement)

*psh*: TCP control flag (push)

*rst*: TCP control flag (reset)

*syn*: TCP control flag (synchronize)

*fin*: TCP control flag (finish)

*udp* – Specifies that the Switch will examine the Universal Datagram Protocol (UDP) field in each packet.

*src\_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.

*dst\_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.

*protocol\_id* <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.

**Parameters**

*port* <portlist> – Specifies the port number on the Switch to permit or deny access for the rule. The user can also configure “all” to specify all ports.

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

## config access\_profile

*priority <value 0-7>* – This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.

*{replace\_priority\_with <value 0-7>}* – Enter this parameter if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

*rx\_rate* – Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation – 64 value = 64kbit/sec. The user may 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.

*delete access\_id <value 1-65535>* – Use this command to delete a specific ACL rule from the Ethernet profile or IP profile. Up to 256 rules may be specified for all access profiles.

### Restrictions

Only Administrator-level users can issue this command.



**NOTE:** Restriction: When the ACL rule is configured, the VLAN and DSCP cant be configured with source IP, destination IP or replace priority it can only be configured with DSCP.

Example usage:

To configure the access profile with the profile ID of 1 to filter frames on port 7 that have IP addresses in the range between 10.42.73.0 to 10.42.73.255:

```
DES-1228/ME:4# config access_profile profile_id 1 add access_id 1 ip source_ip
10.42.73.1 port 7 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1
port 7 deny

Success.

DES-1228/ME:4#
```

## show access\_profile

Purpose	Used to display the currently configured access profiles on the Switch.
Syntax	<b>show access_profile profile_id &lt;value 1-256&gt;</b>
Description	The <b>show access_profile</b> command is used to display the currently configured access profiles.
Parameters	<i>profile_id &lt;value 1-256&gt;</i> – Specify the profile id to display only the access rules configuration for a single profile ID. The user may enter a profile ID number between 1 and 256.
Restrictions	None.

Example usage:

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

```
DES-1228/ME:4#show access_profile
Command: show access_profile

Access Profile Table

=====
Profile ID: 101                               Type: IPv4 Frame Filter - ICMP
=====
Masks  Option
VLAN    Source IP      Dest. IP      DSCP Prot
-----  -
                20.0.0.0      10.0.0.0      ICMP

=====
Total Profile Entries: 1

Total Used Rule Entries: 0

Total Unused Rule Entries: 256

DES-1228/ME:4#
```

## create cpu access\_profile

Purpose	Used to create an access profile specifically for <b>CPU Interface Filtering</b> on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the <b>config cpu access_profile</b> command, below.
Syntax	<b>create cpu access_profile profile_id &lt;value 1-3&gt; [ ethernet { vlan   source_mac &lt;macmask&gt;   destination_mac &lt;macmask&gt;   802.1p   ethernet_type } (1)   ip { vlan   source_ip_mask &lt;netmask&gt;   destination_ip_mask &lt;netmask&gt;   dscp [ [ icmp { type   code }   igmp { type }   tcp {src_port_mask &lt;hex 0x0-0xffff&gt;   dst_port_mask &lt;hex 0x0-0xffff&gt;   flag_mask [ all   {urg   ack   psh   rst   syn   fin}(1)] }   udp {src_port_mask &lt;hex 0x0-0xffff&gt;   dst_port_mask &lt;hex 0x0-0xffff&gt; }   protocol_id_mask &lt;hex 0x0-0xff&gt; {user_define &lt;hex 0x0-0xffffffff&gt;}] (1)]</b>
Description	The <b>create cpu access_profile</b> command is used to create an access profile used only for CPU Interface Filtering. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the <b>config cpu access_profile</b> command, below.
Parameters	<p><i>ethernet</i> – Specifies that the Switch will examine the layer 2 part of each packet header.</p> <ul style="list-style-type: none"> <li><i>vlan</i> – Specifies that the Switch will examine the VLAN part of each packet header.</li> <li><i>source_mac &lt;macmask&gt;</i> – Specifies to examine the source MAC address mask.</li> <li><i>destination_mac &lt;macmask&gt;</i> – Specifies to examine the destination MAC address mask.</li> <li><i>802.1p</i> – Specifies that the Switch will examine the 802.1p priority value in the frame's header.</li> <li><i>ethernet_type</i> – Specifies that the Switch will examine the Ethernet type value in each frame's header.</li> </ul> <p><i>ip</i> – Specifies that the switch will examine the IP address in each frame's header.</p> <p><i>vlan</i> – Specifies a VLAN mask.</p>

**create cpu access\_profile**

*source\_ip\_mask* <netmask> – Specifies an IP address mask for the source IP address.

*destination\_ip\_mask* <netmask> – Specifies an IP address mask for the destination IP address.

*dscp* – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.

*icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.

*type* – Specifies that the Switch will examine each frame's ICMP Type field.

*code* – Specifies that the Switch will examine each frame's ICMP Code field.

*igmp* – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.

*type* – Specifies that the Switch will examine each frame's IGMP Type field.

*tcp* – Specifies that the Switch will examine each frames Transport Control Protocol (TCP) field.

*src\_port\_mask* <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.

*dst\_port\_mask* <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.

*flag\_mask* [ *all* | { *urg* | *ack* | *psh* | *rst* | *syn* | *fin* } ] – Enter the appropriate flag\_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between **all**, **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize) and **fin** (finish).

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

*src\_port\_mask* <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.

*dst\_port\_mask* <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.

*protocol\_id\_mask* <hex 0x0-0xff> – Specifies that the Switch will examine each frame's Protocol ID field using the hex form entered here.

*user\_define\_mask* <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.

*profile\_id* <value 1-3> – Enter an integer between 1 and 3 that is used to identify the CPU access profile to be created with this command.

**Restrictions**

Only Administrator-level users can issue this command.

**Example usage:**

To create a CPU access profile:

```
DES-1228/ME:4# create cpu access_profile profile_id 1 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create cpu access_profile profile_id 1 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code
```

Success.

```
DES-1228/ME:4#
```

## delete cpu access\_profile

Purpose	Used to delete a previously created CPU access profile.
Syntax	<b>delete cpu access_profile profile_id &lt;value 1-3&gt;</b>
Description	The <b>delete cpu access_profile</b> command is used to delete a previously created CPU access profile.
Parameters	<i>profile_id &lt;value 1-3&gt;</i> – 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 <b>create cpu access_profile</b> command.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#delete cpu access_profile profile_id 1
```

```
Command: delete cpu access_profile profile_id 1
```

```
Success.
```

```
DES-1228/ME:4#
```

## config cpu access\_profile

Purpose	Used to configure a CPU access profile used for CPU Interface Filtering and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the <b>create cpu access_profile</b> command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the <b>config cpu access_profile</b> command, below.
Syntax	<b>config cpu access_profile profile_id &lt;value 1-3&gt; [ add access_id &lt;value 1-5&gt; [ ethernet { vlan &lt;vlan_name 32&gt;   source_mac &lt;macaddr&gt;   destination_mac &lt;macaddr&gt;   802.1p &lt;value 0-7&gt;   ethernet_type &lt;hex 0x0-0xffff&gt; }(1)   ip { vlan &lt;vlan_name 32&gt;   source_ip &lt;ipaddr&gt;   destination_ip &lt;ipaddr&gt;   dscp &lt;value 0-63&gt;   [ icmp {type &lt;value 0-255&gt;   code &lt;value 0-255&gt;}   igmp {type &lt;value 0-255&gt;}   tcp {src_port &lt;value 0-65535&gt;   dst_port &lt;value 0-65535&gt;   urg   ack   psh   rst   syn   fin }   udp {src_port &lt;value 0-65535&gt;   dst_port &lt;value 0-65535&gt;}   protocol_id &lt;value 0 - 255&gt; {user_define &lt;hex 0x0-0xffffffff&gt;}}(1)] port [&lt;portlist&gt;   all ][ permit   deny ]   delete access_id &lt;value 1-5&gt; ]</b>
Description	The <b>config cpu access_profile</b> command is used to configure a CPU access profile for CPU Interface Filtering and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the <b>create cpu access_profile</b> command, above.
Parameters	<p><i>profile_id &lt;value 1-3&gt;</i> – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the <b>create access_profile</b> command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority.</p> <p><i>add access_id &lt;value 1-5&gt;</i> – Adds an additional rule to the above specified access profile. The value is used to index the rule created.</p> <p><i>ethernet</i> – Specifies that the Switch will look only into the layer 2 part of each packet.</p> <p><i>vlan &lt;vlan_name 32&gt;</i> – Specifies that the access profile will apply to only to this VLAN.</p> <p><i>source_mac &lt;macaddr&gt;</i> – Specifies that the access profile will apply to this source</p>

**config cpu access\_profile**

MAC address.

*destination\_mac* <macaddr> – Specifies that the access profile will apply to this destination MAC address.

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

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

*vlan* <vlan\_name 32> – Specifies that the access profile will apply to only this VLAN.

*source\_ip* <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address.

*destination\_ip* <ipaddr> – Specifies that the access profile will apply to only packets with this destination IP address.

*dscp* <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header

*icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.

*igmp* – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

*tcp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.

*src\_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.

*dst\_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.

*protocol\_id* <value 0-255> – Specifies that the Switch will examine the Protocol field in each packet and if this field contains the value entered here, apply the following rules.

*udp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.

*src\_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.

*dst\_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.

*protocol\_id* <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.

*user\_define\_mask* <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.

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

*permit* | *deny* – Specify that the packet matching the criteria configured with command will either be permitted entry to the cpu or denied entry to the CPU.

*delete access\_id* <value 1-5> – Use this to remove a previously created access rule in a profile ID.

**Parameters****Restrictions**

Only Administrator-level users can issue this command.

**Example usage:**

To configure CPU access list entry:



```
DES-1228/ME:4#config cpu access_profile profile_id 3 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port all deny
Command: config cpu access_profile profile_id 3 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port all deny
```

Success.

```
DES-1228/ME:4#
```

## delete cpu access\_profile

Purpose	Used to delete a previously created CPU access profile.
Syntax	<b>delete cpu access_profile profile_id &lt;value 1-3&gt;</b>
Description	The <b>delete cpu access_profile</b> command is used to delete a previously created CPU access profile.
Parameters	<i>profile_id &lt;value 1-3&gt;</i> – 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 <b>create cpu access_profile</b> command.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1
```

Success.

```
DES-1228/ME:4#
```

## show cpu access\_profile

Purpose	Used to view the CPU access profile entry currently set in the Switch.
Syntax	<b>show cpu access_profile profile_id &lt;value 1-3&gt;</b>
Description	The <b>show cpu access_profile</b> command is used view the current CPU interface filtering entries set on the Switch.
Parameters	<i>profile_id &lt;value 1-3&gt;</i> – 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 <b>create cpu access_profile</b> command.
Restrictions	None.

Example usage:

To show the CPU filtering state on the Switch:

```
DES-1228/ME:4#show cpu access_profile profile_id 2
Command: show cpu access_profile profile_id 2

CPU Interface Filtering state: Disabled

Access Profile Table
=====
Total Profile Entries: 0
Total Rule Entries: 0

DES-1228/ME:4#
```

## enable cpu\_interface\_filtering

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

Example Usage:

To enable CPU interface filtering:

```
DES-1228/ME:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-1228/ME:4#
```

## disable cpu\_interface\_filtering

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

Example Usage:

To disable CPU filtering:

```
DES-1228/ME:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-1228/ME:4#
```

## SAFEGUARD ENGINE COMMANDS

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

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

It will limit bandwidth of receiving ARP packets.

It will limit the bandwidth of IP packets received by the Switch.

IP packets may also be limited by the Switch by configuring only certain IP addresses to be accepted. This method can be accomplished through the `create trusted_host` explained in the previous section. Once the user configures these acceptable IP addresses, other packets containing different IP addresses will be dropped by the Switch, thus limiting the bandwidth of IP packets

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

Command	Parameters
<code>config safeguard_engine</code>	{state [enable disable]  utilization { rising <value 20-100>  falling <value 20-100>}(1)   trap_log [enable disable]  mode [ strict   fuzzy] }(1)
<code>show safeguard_engine</code>	

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

### config safeguard\_engine

Purpose	To configure ARP storm control for system.
Syntax	<b>config safeguard_engine {state [enable disable]  utilization { rising &lt;value 20-100&gt;  falling &lt;value 20-100&gt;}(1)   trap_log [enable disable]  mode [ strict   fuzzy] }(1)</b>
Description	Use this command to configure Safeguard Engine to minimize the effects of an ARP storm.
Parameters	<p><i>state [enable   disable]</i> – Select the running state of the Safeguard Engine function as enable or disable.</p> <p><i>cpu_utilization</i> – Select this option to trigger the Safeguard Engine function to enable based on the following determinates:</p> <p><i>rising &lt;value 20-100&gt;</i> – The user can set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises to this percentage, the Safeguard Engine mechanism will initiate.</p> <p><i>falling &lt;value 20-100&gt;</i> – The user can set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to this percentage, the Safeguard Engine mechanism will shut down.</p> <p><i>trap_log [enable   disable]</i> – Choose whether to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.</p> <p><i>mode [strict   fuzzy]</i> – Toggle between <i>strict</i> and <i>fuzzy</i> mode.</p> <p><i>strict</i> – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided.</p> <p><i>fuzzy</i> – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the safeguard engine for the Switch:

```
DES-1228/ME:4#config safeguard_engine state enable utilization rising 45
Command: config safeguard_engine state enable utilization rising 45

Success.

DES-1228/ME:4#
```

## show safeguard\_engine

Purpose	Used to display current Safeguard Engine settings.
Syntax	<b>show safeguard_engine</b>
Description	This will list the current status and type of the Safeguard Engine settings currently configured.
Parameters	None.
Restrictions	None.

Example usage:

To display the safeguard engine status:

```
DES-1228/ME:4#show safeguard_engine
Command: show safeguard_engine

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

DES-1228/ME:4#
```

## TRAFFIC SEGMENTATION COMMANDS

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

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

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

### config traffic\_segmentation

Purpose	Used to configure traffic segmentation on the Switch.
Syntax	<b>config traffic_segmentation</b> <portlist> forward_list [null   <portlist>]
Description	The <b>config traffic_segmentation</b> command is used to configure traffic segmentation on the Switch.
Parameters	<p>&lt;portlist&gt; – Specifies a port or range of ports that will be configured for traffic segmentation.</p> <p>forward_list – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.</p> <ul style="list-style-type: none"> <li>• <i>null</i> – No ports are specified</li> <li>• &lt;portlist&gt; – Specifies a range of ports for the forwarding list. This list must be on the same Switch previously specified for traffic segmentation (i.e. following the &lt;portlist&gt; specified above for <b>config traffic_segmentation</b>).</li> </ul>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DES-1228/ME:4#
```

### show traffic\_segmentation

Purpose	Used to display the current traffic segmentation configuration on the Switch.
Syntax	<b>show traffic_segmentation</b> <portlist>
Description	The <b>show traffic_segmentation</b> command is used to display the current traffic segmentation configuration on the Switch.
Parameters	<portlist> – Specifies a port or range of ports for which the current traffic segmentation configuration on the Switch will be displayed.
Restrictions	The port lists for segmentation and the forward list must be on the same Switch.

Example usage:

To display the current traffic segmentation configuration on the Switch.

```
DES-1228/ME:4#show traffic_segmentation
```

```
Command: show traffic_segmentation
```

```
Traffic Segmentation Table
```

```
Port      Forward Portlist
```

```
-----
```

```
1         1-28
```

```
2         1-28
```

```
3         1-28
```

```
4         1-28
```

```
5         1-28
```

```
6         1-28
```

```
7         1-28
```

```
8         1-28
```

```
9         1-28
```

```
10        1-28
```

```
11        1-28
```

```
12        1-28
```

```
13        1-28
```

```
14        1-28
```

```
15        1-28
```

```
16        1-28
```

```
17        1-28
```

```
18        1-28
```

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

## TIME AND SNTP COMMANDS

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

Command	Parameters
config sntp	{primary <ipaddr>   secondary <ipaddr>   poll-interval <int 30-99999>}(1)
show sntp	
enable sntp	
disable sntp	
config time	<date ddmmyyyy > <time hh:mm:ss >
config time_zone	{operator [+ -]   hour <gmt_hour 0-13>   min <minute 0-59>}(3)
config dst	[disable   repeating {s_week <start_week 1-5,last>   s_day <start_day sun-sat>   s_mth <start_mth 1-12>   s_time <start_time hh:mm>   e_week <end_week 1-5,last>   e_day <end_day sun-sat>   e_mth <end_mth 1-12>   e_time <end_time hh:mm>   offset [30 60 90 120]}(9)   annual {s_date <start_date 1-31>   s_mth <start_mth 1-12>   s_time <start_time hh:mm>   e_date <end_date 1-31>   e_mth <end_mth 1-12>   e_time <end_time hh:mm>   offset [30 60 90 120]}(7)]
show time	

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

### config sntp

Purpose	Used to setup SNTP service.
Syntax	<b>config sntp {primary &lt;ipaddr&gt;   secondary &lt;ipaddr&gt;   poll-interval &lt;int 30-99999&gt;}(1)</b>
Description	Use this command to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable sntp).
Parameters	<p><i>primary</i> – This is the primary server from which the SNTP information will be taken.</p> <p><i>&lt;ipaddr&gt;</i> – The IP address of the primary server.</p> <p><i>secondary</i> – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <p><i>&lt;ipaddr&gt;</i> – The IP address for the secondary server.</p> <p><i>poll-interval &lt;int 30-99999&gt;</i> – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.</p>
Restrictions	Only Administrator-level users can issue this command. SNTP service must be enabled for this command to function ( <i>enable sntp</i> ).

Example usage:

To configure SNTP settings:

```
DES-1228/ME:4#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DES-1228/ME:4#
```

## show sntp

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

Example usage:

To display SNTP configuration information:

```
DES-1228/ME:4#show sntp
Command: show sntp

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

DES-1228/ME:4#
```

## enable sntp

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

Example usage:

To enable the SNTP function:

```
DES-1228/ME:4#enable sntp
Command: enable sntp

Success.

DES-1228/ME:4#
```



## disable sntp

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

Example usage:

To disable SNTP support:

```
DES-1228/ME:4#disable sntp
```

```
Command: disable sntp
```

```
Success.
```

```
DES-1228/ME:4#
```

## config time

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

Example usage:

To manually set system time and date settings:

```
DES-1228/ME:4#config time 30jun2003 16:30:30
```

```
Command: config time 30jun2003 16:30:30
```

```
Success.
```

```
DES-1228/ME:4#
```

## config time\_zone

Purpose	Used to determine the time zone used in order to adjust the system clock.
Syntax	<b>config time_zone {operator [+ -]   hour &lt;gmt_hour 0-13&gt;   min &lt;minute 0-59&gt;}(3)</b>
Description	This will adjust system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	<i>operator</i> – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT.

**config time\_zone**

*hour* – Select the number of hours different from GMT.

*min* – Select the number of minutes difference added or subtracted to adjust the time zone.

Restrictions                      Only Administrator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DES-1228/ME:4#config time_zone operator + hour 2 min 30
```

```
Command: config time_zone operator + hour 2 min 30
```

```
Success.
```

```
DES-1228/ME:4#
```

**config dst**

Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	<b>config dst [disable   repeating {s_week &lt;start_week 1-5,last&gt;   s_day &lt;start_day sun-sat&gt;   s_mth &lt;start_mth 1-12&gt;   s_time &lt;start_time hh:mm&gt;   e_week &lt;end_week 1-5,last&gt;   e_day &lt;end_day sun-sat&gt;   e_mth &lt;end_mth 1-12&gt;   e_time &lt;end_time hh:mm&gt;   offset [30 60 90 120]}(9)   annual {s_date &lt;start_date 1-31&gt;   s_mth &lt;start_mth 1-12&gt;   s_time &lt;start_time hh:mm&gt;   e_date &lt;end_date 1-31&gt;   e_mth &lt;end_mth 1-12&gt;   e_time &lt;end_time hh:mm&gt;   offset [30 60 90 120]}(7)]</b>
Description	<p>DST can be enabled and configured using this command. When enabled this will adjust the system clock to comply with any DST requirement. DST adjustment effects system time for both manually configured time and time set using SNTP service.</p> <p><i>disable</i> – Disable the DST seasonal time adjustment for the Switch.</p> <p><i>repeating</i> – Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.</p> <p><i>annual</i> – Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.</p> <p><i>s_week</i> – Configure the week of the month in which DST begins.</p> <ul style="list-style-type: none"> <li>• <i>&lt;start_week 1-4,last&gt;</i> – The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month.</li> </ul> <p><i>e_week</i> – Configure the week of the month in which DST ends.</p> <ul style="list-style-type: none"> <li>• <i>&lt;end_week 1-4,last&gt;</i> – The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month.</li> </ul> <p><i>s_day</i> – Configure the day of the week in which DST begins.</p> <ul style="list-style-type: none"> <li>• <i>&lt;start_day sun-sat&gt;</i> – The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)</li> </ul> <p><i>e_day</i> – Configure the day of the week in which DST ends.</p> <ul style="list-style-type: none"> <li>• <i>&lt;end_day sun-sat&gt;</i> – The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)</li> </ul> <p><i>s_mth</i> – Configure the month in which DST begins.</p> <ul style="list-style-type: none"> <li>• <i>&lt;start_mth 1-12&gt;</i> – The month to begin DST expressed as a number.</li> </ul> <p><i>e_mth</i> – Configure the month in which DST ends.</p> <ul style="list-style-type: none"> <li>• <i>&lt;end_mth 1-12&gt;</i> – The month to end DST expressed as a number.</li> </ul> <p><i>s_time</i> – Configure the time of day to begin DST.</p> <ul style="list-style-type: none"> <li>• <i>&lt;start_time hh:mm&gt;</i> – Time is expressed using a 24-hour clock, in hours and minutes.</li> </ul>
Parameters	<ul style="list-style-type: none"> <li>• <i>&lt;end_week 1-4,last&gt;</i> – The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month.</li> </ul>

## config dst

*e\_time* – Configure the time of day to end DST.

- *<end\_time hh:mm>* – Time is expressed using a 24-hour clock, in hours and minutes.

*s\_date* – Configure the specific date (day of the month) to begin DST.

- *<start\_date 1-31>* – The start date is expressed numerically.

*e\_date* – Configure the specific date (day of the month) to begin DST.

- *<end\_date 1-31>* – The end date is expressed numerically.

*offset [30 | 60 | 90 | 120]* – Indicates number of minutes to add or to subtract during the summertime. The possible offset times are 30,60,90,120. The default value is 60

Restrictions

Only Administrator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DES-1228/ME:4#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30
```

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

Success.

```
DES-1228/ME:4#
```

## show time

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

Example usage:

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

```
DES-1228/ME:4#show time
```

```
Command: show time
```

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

```
DES-1228/ME:4#
```

## ARP COMMANDS

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

Command	Parameters
create arprentry	<ipaddr> <macaddr>
config arprentry	<ipaddr> <macaddr>
delete arprentry	{[<ipaddr>   all]}
show arprentry	{ipif [System]   ipaddress <ipaddr>   static}
config arp_aging time	<value 0-65535>
clear arptable	

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

### create arprentry

Purpose	Used to make a static entry into the ARP table.
Syntax	<b>create arprentry &lt;ipaddr&gt; &lt;macaddr&gt;</b>
Description	This command is used to enter an IP address and the corresponding MAC address into the Switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. <macaddr> – The MAC address corresponding to the IP address above.
Restrictions	Only Administrator-level users can issue this command. The Switch supports up to 255 static ARP entries.

Example Usage:

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

```
DES-1228/ME:4#create arprentry 10.48.74.121 00-50-BA-00-07-36
Command: create arprentry 10.48.74.121 00-50-BA-00-07-36

Success.

DES-1228/ME:4#
```

### config arprentry

Purpose	Used to configure a static entry in the ARP table.
Syntax	<b>config arprentry &lt;ipaddr&gt; &lt;macaddr&gt;</b>
Description	This command is used to configure a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the Switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. <macaddr> – The MAC address corresponding to the IP address above.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

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

```
DES-1228/ME:4#config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

Success.

DES-1228/ME:4#
```

## delete arpentry

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

Example Usage:

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

```
DES-1228/ME:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DES-1228/ME:4#
```

## config arp\_aging time

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

Example Usage:

To configure ARP aging time:

```
DES-1228/ME:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DES-1228/ME:4#
```

**show arpentry**

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

Example Usage:

To display the ARP table:

```
DES-1228/ME:4#show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface      IP Address      MAC Address      Type
-----
System         10.0.0.0        FF-FF-FF-FF-FF-FF Local/Broadcast
System         10.6.51.15      00-1D-60-E7-B5-CD Dynamic
System         10.22.8.50      00-80-C8-DF-E8-EE Dynamic
System         10.30.28.112    00-30-28-01-12-02 Dynamic
System         10.39.77.24     08-00-01-43-00-00 Dynamic
System         10.44.8.253     00-44-08-FD-09-09 Dynamic
System         10.53.7.12      00-50-BA-11-11-04 Dynamic
System         10.56.85.10     00-0E-A6-8F-72-EA Dynamic
System         10.67.33.67     00-00-E2-58-DB-CF Dynamic
System         10.71.77.126    00-04-96-20-D5-25 Dynamic
System         10.73.21.11     00-19-5B-EF-78-B5 Local
System         10.73.60.106    00-00-00-11-12-13 Dynamic
System         10.90.90.90     00-21-91-21-34-03 Dynamic
System         10.255.255.255  FF-FF-FF-FF-FF-FF Local/Broadcast

Total Entries  : 14

DES-1228/ME:4#
```

**clear arptable**

Purpose	Used to remove all dynamic ARP table entries.
Syntax	<b>clear arptable</b>
Description	This command is used to remove dynamic ARP table entries from the Switch's ARP table. Static ARP table entries are not affected.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
DES-1228/ME:4#clear arptable
Command: clear arptable

Success.

DES-1228/ME:4#
```



## ROUTING TABLE COMMANDS

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

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

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

### create iproute default

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

Example usage:

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

```
DES-1228/ME:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DES-1228/ME:4#
```

### delete iproute default

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

Example usage:

To delete the default IP route 10.53.13.254:

```
DES-1228/ME:4#delete iproute default 10.53.13.254
```

```
Command: delete iproute default 10.53.13.254
```

```
Success.
```

```
DES-1228/ME:4#
```

## show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	<b>show iproute {&lt;network_address&gt;   static}</b>
Description	This command will display the Switch's current IP routing table.
Parameters	<network_address> – The network IP address. static – Select a static IP route.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DES-1228/ME:4#show iproute
```

```
Command: show iproute
```

```
Routing Table
```

IP Address/Netmask	Gateway	Interface	Hops	Protocol
0.0.0.0	10.1.1.254	System	1	Default
10.0.0.0/8	10.48.74.122	System	1	Local

```
Total Entries: 2
```

```
DES-1228/ME:4#
```

## MAC NOTIFICATION COMMANDS

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

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

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

### enable mac\_notification

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

Example usage:

To enable MAC notification without changing basic configuration:

```
DES-1228/ME:4#enable mac_notification
```

```
Command: enable mac_notification
```

```
Success.
```

```
DES-1228/ME:4#
```

### disable mac\_notification

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

Example usage:

To disable MAC notification without changing basic configuration:

```
DES-1228/ME:4#disable mac_notification
```

```
Command: disable mac_notification
```

```
Success.
```

```
DES-1228/ME:4#
```

## config mac\_notification

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

Example usage:

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

```
DES-1228/ME:4#config mac_notification interval 1 historysize 500
```

```
Command: config mac_notification interval 1 historysize 500
```

```
Success.
```

```
DES-1228/ME:4#
```

## config mac\_notification ports

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

Example usage:

To enable port 7 for MAC address table notification:

```
DES-1228/ME:4#config mac_notification ports 7 enable
```

```
Command: config mac_notification ports 7 enable
```

```
Success.
```

```
DES-1228/ME:4#
```

## show mac\_notification

Purpose	Used to display the Switch's MAC address table notification global settings.
Syntax	<b>show mac_notification</b>
Description	This command is used to display the Switch's MAC address table notification global settings.
Parameters	None.
Restrictions	None.

Example usage:

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

```
DES-1228/ME:4#show mac_notification
```

```
Command: show mac_notification
```

### Global Mac Notification Settings

```
State          : Enabled
```

```
Interval       : 1
```

```
History Size   : 1
```

```
DES-1228/ME:4#
```

## show mac\_notification ports

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

Example usage:

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

```
DES-1228/ME:4#show mac_notification ports
```

```
Command: show mac_notification ports
```

```
Port #  MAC Address Table Notification State
```

```
-----  -----
```

1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled

10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled

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

## ACCESS AUTHENTICATION CONTROL COMMANDS

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

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

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

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

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

- A) The server verifies the username and password, and the user is granted normal user privileges on the Switch.
- B) The server will not accept the username and password and the user is denied access to the Switch.
- C) The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

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

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

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



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

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

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

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



## enable authen\_policy

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

Example usage:

To enable the system access authentication policy:

```
DES-1228/ME:4#enable authen_policy
```

```
Command: enable authen_policy
```

```
Success.
```

```
DES-1228/ME:4#
```

## disable authen\_policy

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

Example usage:

To disable the system access authentication policy:

```
DES-1228/ME:4#disable authen_policy
```

```
Command: disable authen_policy
```

```
Success.
```

```
DES-1228/ME:4#
```

## show authen\_policy

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

Example usage:

To display the system access authentication policy:

```
DES-1228/ME:4#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DES-1228/ME:4#
```

## create authen\_login method\_list\_name

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

Example usage:

To create the method list “Trinity.”:

```
DES-1228/ME:4#create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity

Success.

DES-1228/ME:4#
```

## config authen\_login

Purpose	Used to configure a user-defined or default <i>method list</i> of authentication methods for user login.
Syntax	<b>config authen_login [default   method_list_name &lt;string 15&gt;] method {tacacs   xtacacs   tacacs+   radius   server_group &lt;string 15&gt;   local   none}(1)</b>
Description	<p>This command will configure a user-defined or default <i>method list</i> of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like <i>tacacs – xtacacs – local</i>, the Switch will send an authentication request to the first <i>tacacs</i> host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second <i>tacacs</i> host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, <i>xtacacs</i>. If no authentication takes place using the <i>xtacacs</i> list, the <i>local</i> account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.</p> <p>Successful login using any of these methods will give the user a “user” privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the <i>enable admin</i> command, followed by a previously configured password. (See the <b>enable admin</b> part of this section for more detailed information, concerning the <b>enable admin</b> command.)</p>
Parameters	<i>default</i> – The default method list for access authentication, as defined by the user. The

## config\_authen\_login

user may choose one or a combination of up to four(4) of the following authentication methods:

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

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

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



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

### Restrictions

Only Administrator-level users can issue this command.

### Example usage:

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

```
DES-1228/ME:4#config_authen_login method_list_name Trinity method tacacs xtacacs local
Command: config_authen_login method_list_name Trinity method tacacs xtacacs local
```

Success.

```
DES-1228/ME:4#
```

### Example usage:

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

```
DES-1228/ME:4#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

DES-1228/ME:4#
```

## delete authen\_login method\_list\_name

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

Example usage:

To delete the method list name “Trinity”:

```
DES-1228/ME:4#delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DES-1228/ME:4#
```

## show authen\_login

Purpose	Used to display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	<b>show authen_login [default   method_list_name &lt;string 15&gt;   all]</b>
Description	This command is used to show a list of authentication methods for user login.
Parameters	<p><i>default</i> – Entering this parameter will display the default method list for users logging on to the Switch.</p> <p><i>method_list_name &lt;string 15&gt;</i> – Enter an alphanumeric string of up to 15 characters to define the given <i>method list</i> to view.</p> <p><i>all</i> – Entering this parameter will display all the authentication login methods currently configured on the Switch.</p> <p>The window will display the following parameters:</p> <ul style="list-style-type: none"> <li>▪ Method List Name – The name of a previously configured method list name.</li> <li>▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest).</li> <li>▪ Method Name – Defines which security protocols are implemented, per method list name.</li> <li>▪ Comment – Defines the type of Method. <i>User-defined Group</i> refers to server group defined by the user. <i>Built-in Group</i> refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. <i>Keyword</i> refers to authentication using a technique INSTEAD of TACACS / XTACACS / TACACS+ / RADIUS which are local (authentication through the</li> </ul>

## show authen\_login

user account on the Switch) and none (no authentication necessary to access any function on the Switch).

Restrictions               None.

Example usage:

To view the authentication login method list named Trinity:

```
DES-1228/ME:4#show authen_login method_list_name Trinity
Command: show authen_login method_list_name Trinity

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

DES-1228/ME:4#
```

## create authen\_enable method\_list\_name

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

Example usage:

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

```
DES-1228/ME:4#create authen_enable method_list_name Permit
Command: create authen_enable method_list_name Permit

Success.

DES-1228/ME:4#
```

## config authen\_enable

Purpose	Used to configure a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	<b>config authen_enable [default   method_list_name &lt;string 15&gt;] method {tacacs   xtacacs   tacacs+   radius   server_group &lt;string 15&gt;   local_enable   none}(1)</b>
Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user

**config authen\_enable**

level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented simultaneously on the Switch.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs* – *xtacacs* – *local\_enable*, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local\_enable* password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an “Admin” level privilege.

## Parameters

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

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

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

- *tacacs* – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.
- *xtacacs* – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.
- *tacacs+* – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.
- *radius* – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.
- *server\_group* <*string 15*> – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.
- *local\_enable* – Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch. The local enable password of the device can be configured using the “**config admin local\_password**” command.
- *none* – Adding this parameter will require no authentication to access the administration level privileges on the Switch.

## Restrictions

Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#config authn_enable method_list_name Trinity method tacacs xtacacs local
Command: config authn_enable method_list_name Trinity method tacacs xtacacs local

Success.

DES-1228/ME:4#
```

Example usage:

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

```
DES-1228/ME:4#config authn_enable default method xtacacs tacacs+ local
Command: config authn_enable default method xtacacs tacacs+ local

Success.

DES-1228/ME:4#
```

## delete authn\_enable method\_list\_name

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

Example usage:

To delete the user-defined method list “Permit”

```
DES-1228/ME:4#delete authn_enable method_list_name Permit
Command: delete authn_enable method_list_name Permit

Success.

DES-1228/ME:4#
```

## show authn\_enable

Purpose	Used to display the method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	<b>show authn_enable [default   method_list_name &lt;string 15&gt;   all]</b>
Description	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	<i>default</i> – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the Switch. <i>method_list_name &lt;string 15&gt;</i> – Enter an alphanumeric string of up to 15 characters to define the given <i>method list</i> the user wishes to view.

## show authen\_enable

all – Entering this parameter will display all the authentication login methods currently configured on the Switch.

The window will display the following parameters:

- Method List Name – The name of a previously configured method list name.
- Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest).
- Method Name – Defines which security protocols are implemented, per method list name.
- Comment – Defines the type of Method. *User-defined Group* refers to *server groups* defined by the user. *Built-in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the *local\_enable* password on the Switch) and none (no authentication necessary to access any function on the Switch).

Restrictions                      None.

Example usage:

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

```
DES-1228/ME:4#show authen_enable all
```

```
Command: show authen_enable all
```

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

```
Total Entries : 2
```

```
DES-1228/ME:4#
```

## config authen application

**Purpose**                      Used to configure various applications on the Switch for authentication using a previously configured method list.

**Syntax**                      **config authen application [console | telnet | ssh | http | all] [login | enable] [default | method\_list\_name <string 15>]**

**Description**                This command is used to configure Switch configuration applications (console, telnet, ssh, web) for login at the user level and at the administration level (*authen\_enable*) utilizing a previously configured method list.

**Parameters**                *application* – Choose the application to configure. The user may choose one of the following five options to configure.

- *console* – Choose this parameter to configure the command line interface login method.
- *telnet* – Choose this parameter to configure the telnet login method.



## config authen application

- *ssh* – Choose this parameter to configure the Secure Shell login method.
- *http* – Choose this parameter to configure the web interface login method.
- *all* – Choose this parameter to configure all applications (console, telnet, ssh, web) login method.

*login* – Use this parameter to configure an application for normal login on the user level, using a previously configured method list.

*enable* – Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list.

*default* – Use this parameter to configure an application for user authentication using the default method list.

*method\_list\_name* <string 15> – Use this parameter to configure an application for user authentication using a previously configured method list. Enter an alphanumeric string of up to 15 characters to define a previously configured method list.

### Restrictions

Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the web interface:

```
DES-1228/ME:4#config authen application http login default
```

```
Command: config authen application http login default
```

Success.

```
DES-1228/ME:4#
```

## show authen application

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

Example usage:

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

```
DES-1228/ME:4#show authen application
```

```
Command: show authen application
```

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

```
DES-1228/ME:4#
```

**create authen server\_host**

Purpose	Used to create an authentication server host.
Syntax	<b>create authen server_host &lt;ipaddr&gt; protocol [tacacs   xtacacs   tacacs+   radius] {port &lt;int 1-65535&gt;   key [&lt;key_string 254&gt;   none]   timeout &lt;int 1-255&gt;   retransmit &lt; 1-255&gt;}</b>
Description	This command will create an authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	<p><i>server_host &lt;ipaddr&gt;</i> – The IP address of the remote server host to add.</p> <p><i>protocol</i> – The protocol used by the server host. The user may choose one of the following:</p> <ul style="list-style-type: none"> <li>▪ <i>tacacs</i> – Enter this parameter if the server host utilizes the TACACS protocol.</li> <li>▪ <i>xtacacs</i> – Enter this parameter if the server host utilizes the XTACACS protocol.</li> <li>▪ <i>tacacs+</i> – Enter this parameter if the server host utilizes the TACACS+ protocol.</li> <li>▪ <i>radius</i> – Enter this parameter if the server host utilizes the RADIUS protocol.</li> </ul> <p><i>port &lt;int 1-65535&gt;</i> – Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.</p> <p><i>key &lt;key_string 254&gt;</i> – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters.</p> <p><i>timeout &lt;int 1-255&gt;</i> – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.</p> <p><i>retransmit &lt;int 1-255&gt;</i> – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond.</p>
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-1228/ME:4#create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5
```

```
Command: create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5
```

Success.

```
DES-1228/ME:4#
```

**config authen server\_host**

Purpose	Used to configure a user-defined authentication server host.
Syntax	<b>config authen server_host &lt;ipaddr&gt; protocol [tacacs   xtacacs   tacacs+   radius] {port &lt;int 1-65535&gt;   key [&lt;key_string 254&gt;   none]   timeout &lt;int 1-255&gt;   retransmit &lt;int 1-255&gt;}(1)</b>
Description	This command will configure a user-defined authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user

## config authen server\_host

attempts to access the Switch with the authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

### Parameters

*server\_host* <ipaddr> – The IP address of the remote server host the user wishes to alter.  
*protocol* – The protocol used by the server host. The user may choose one of the following:

- *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol.
- *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol.
- *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol.
- *radius* – Enter this parameter if the server host utilizes the RADIUS protocol.

*port* <int 1-65535> – Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.

*key* <key\_string 254> – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters or choose none.

*timeout* <int 1-255> – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.

*retransmit* <int 1-255> – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond. This field is inoperable for the TACACS+ protocol.

### Restrictions

Only Administrator-level users can issue this command.

### Example usage:

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

```
DES-1228/ME:4#config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12 retransmit 4
```

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

Success.

```
DES-1228/ME:4#
```

## delete authen server\_host

### Purpose

Used to delete a user-defined authentication server host.

### Syntax

**delete authen server\_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**

### Description

This command is used to delete a user-defined authentication server host previously created on the Switch.

### Parameters

*server\_host* <ipaddr> – The IP address of the remote server host to be deleted.

*protocol* – The protocol used by the server host the user wishes to delete. The user may choose one of the following:

- *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol.
- *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol.

## delete authn server\_host

- *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol.
- *radius* – Enter this parameter if the server host utilizes the RADIUS protocol.

Restrictions Only Administrator-level users can issue this command.

Example usage:

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

```
DES-1228/ME:4#delete authn server_host 10.1.1.121 protocol tacacs+
```

```
Command: delete authn server_host 10.1.1.121 protocol tacacs+
```

Success.

```
DES-1228/ME:4#
```

## show authn server\_host

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

Example usage:

To view authentication server hosts currently set on the Switch:

```
DES-1228/ME:4#show authn server_host
```

```
Command: show authn server_host
```

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

```
Total Entries : 1
```

```
DES-1228/ME:4#
```

## create authn server\_group

Purpose	Used to create a user-defined authentication server group.
---------	--

## create authen server\_group

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

Example usage:

To create the server group “group\_1”:

```
DES-1228/ME:4#create authen server_group group_1
```

```
Command: create authen server_group group_1
```

**Success.**

```
DES-1228/ME:4#
```

**config authen server\_group**

Purpose	Used to configure a user-defined authentication server group.
Syntax	<b>config authen server_group [tacacs   xtacacs   tacacs+   radius   &lt;string 15&gt;] [add   delete] server_host &lt;ipaddr&gt; protocol [tacacs   xtacacs   tacacs+   radius]</b>
Description	This command will configure an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. Up to eight authentication server hosts may be added to any particular group
Parameters	<p><i>server_group</i> – The user may define the group by protocol groups built into the Switch (TACACS/XTACACS/TACACS+/RADIUS), or by a user-defined group previously created using the <i>create authen server_group</i> command.</p> <ul style="list-style-type: none"> <li>▪ <i>tacacs</i> – Use this parameter to utilize the built-in TACACS server protocol on the Switch. Only server hosts utilizing the TACACS protocol may be added to this group.</li> <li>▪ <i>xtacacs</i> – Use this parameter to utilize the built-in XTACACS server protocol on the Switch. Only server hosts utilizing the XTACACS protocol may be added to this group.</li> <li>▪ <i>tacacs+</i> – Use this parameter to utilize the built-in TACACS+ server protocol on the Switch. Only server hosts utilizing the TACACS+ protocol may be added to this group.</li> <li>▪ <i>radius</i> – Use this parameter to utilize the built-in RADIUS server protocol on the Switch. Only server hosts utilizing the RADIUS protocol may be added to this group.</li> <li>▪ <i>&lt;string 15&gt;</i> – Enter an alphanumeric string of up to 15 characters to define the previously created server group. This group may add any combination of server hosts to it, regardless of protocol.</li> </ul> <p><i>add/delete</i> – Enter the correct parameter to add or delete a server host from a server group.</p> <p><i>server_host &lt;ipaddr&gt;</i> – Enter the IP address of the previously configured server host to add or delete.</p> <p><i>protocol</i> – Enter the protocol utilized by the server host. There are three options:</p> <ul style="list-style-type: none"> <li>▪ <i>tacacs</i> – Use this parameter to define the protocol if the server host is using the TACACS authentication protocol.</li> <li>▪ <i>xtacacs</i> – Use this parameter to define the protocol if the server host is using the XTACACS authentication protocol.</li> <li>▪ <i>tacacs+</i> – Use this parameter to define the protocol if the server host is using the TACACS+ authentication protocol.</li> <li>▪ <i>radius</i> – Use this parameter to define the protocol if the server host is using the RADIUS authentication protocol.</li> </ul>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add an authentication host to server group “group\_1”:

```
DES-1228/ME:4# config authen server_group group_1 add server_host 10.1.1.121 protocol tacacs+
Command: config authen server_group group_1 add server_host 10.1.1.121 protocol tacacs+

Success.

DES-1228/ME:4#
```

**delete authen server\_group**

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

Example usage:

To delete the server group “group\_1”:

```
DES-1228/ME:4#delete server_group group_1
```

```
Command: delete server_group group_1
```

```
Success.
```

```
DES-1228/ME:4#
```

**show authen server\_group**

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

Example usage:

To view authentication server groups currently set on the Switch.

```
DES-1228/ME:4#show authen server_group
```

```
Command: show authen server_group
```

```

Group Name      IP Address      Protocol
-----
radius          -----
tacacs          -----
tacacs+         -----
xtacacs         -----

```

```
Total Entries : 4
```

```
DES-1228/ME:4#
```

**config authen parameter response\_timeout**

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

Example usage:

To configure the response timeout for 60 seconds:

```
DES-1228/ME:4#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60
```

Success.

```
DES-1228/ME:4#
```

**config authen parameter attempt**

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

Example usage:

To set the maximum number of authentication attempts at 5:

```
DES-1228/ME:4#config authen parameter attempt 5
Command: config authen parameter attempt 5
```

Success.

```
DES-1228/ME:4#
```

**show authen parameter**

Purpose	Used to display the authentication parameters currently configured on the Switch.
Syntax	<b>show authen parameter</b>



## show authen parameter

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

Example usage:

To view the authentication parameters currently set on the Switch:

```
DES-1228/ME:4#show authen parameter
```

```
Command: show authen parameter
```

```
Response Timeout : 60 seconds
```

```
User Attempts      : 5
```

```
DES-1228/ME:4#
```

## enable admin

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

Example usage:

To enable administrator privileges on the Switch:

```
DES-1228/ME:4#enable admin
```

```
Password: *****
```

```
DES-1228/ME:4#
```

## config admin local\_enable

Purpose	Used to configure the local enable password for administrator level privileges.
Syntax	<b>config admin local_enable</b>
Description	This command will configure the locally enabled password for the <b>enable admin</b>

## config admin local\_enable

	command. When a user chooses the “ <i>local_enable</i> ” method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is set locally on the Switch.
Parameters	< <i>password 15</i> > – After entering this command, the user will be prompted to enter the old password, then a new password in an alphanumeric string of no more than 15 characters, and finally prompted to enter the new password again for confirmation. See the example below.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the password for the “local\_enable” authentication method.

```
DES-1228/ME:4#config admin local_enable
```

```
Command: config admin local_enable
```

```
Enter the old password:
```

```
Enter the case-sensitive new password:*****
```

```
Enter the new password again for confirmation:*****
```

```
Success.
```

```
DES-1228/ME:4#
```

## SSH COMMANDS

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

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

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

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

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

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

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

Command	Parameters
enable ssh	
disable ssh	
config ssh authmode	[password   publickey   hostbased] [enable   disable]
show ssh authmode	
config ssh server	{maxsession <int 1-8>   contimeout <sec 120-600>   authfail<int 2-20>   rekey [ 10min   30min   60min   never] }(1)
show ssh server	
config ssh user	<username 15> authmode [hostbased [hostname <domain_name 32>   hostname_IP <domain_name 32> <ipaddr>]   password   publickey]
show ssh user authmode	
config ssh algorithm	[3DES   AES128   AES192   AES256   arcfour   blowfish   cast128   twofish128   twofish192   twofish256   MD5   SHA1   RSA   DSA] [enable   disable]
show ssh algorithm	
config ssh regenerate hostkey	

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

**enable ssh**

Purpose	Used to enable SSH.
Syntax	<b>enable ssh</b>
Description	This command allows users to enable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To enable SSH:

```
DES-1228/ME:4#enable ssh
```

```
Command: enable ssh
```

```
Success.
```

```
DES-1228/ME:4#
```

**disable ssh**

Purpose	Used to disable SSH.
Syntax	<b>disable ssh</b>
Description	This command allows users to disable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To disable SSH:

```
DES-1228/ME:4# disable ssh
```

```
Command: disable ssh
```

```
Success.
```

```
DES-1228/ME:4#
```

**config ssh authmode**

Purpose	Used to configure the SSH authentication mode setting.
Syntax	<b>config ssh authmode [password   publickey   hostbased] [enable   disable]</b>
Description	This command will allow users to configure the SSH authentication mode for users attempting to access the Switch.

## config ssh authmode

Parameters	<p><i>password</i> – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the Switch.</p> <p><i>publickey</i> – This parameter may be chosen if the administrator wishes to use a publickey configuration set on a SSH server, for authentication.</p> <p><i>hostbased</i> – This parameter may be chosen if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed.</p> <p><i>[enable   disable]</i> – This allows users to enable or disable SSH authentication on the Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DES-1228/ME:4#config ssh authmode password enable
```

```
Command: config ssh authmode password enable
```

Success.

```
DES-1228/ME:4#
```

## show ssh authmode

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

Example usage:

To view the current authentication mode set on the Switch:

```
DES-1228/ME:4#show ssh authmode
```

```
Command: show ssh authmode
```

The SSH authmode:

```
Password      : Enabled
```

```
Publickey     : Enabled
```

```
Hostbased     : Enabled
```

```
DES-1228/ME:4#
```

## config ssh server

Purpose	Used to configure the SSH server.
Syntax	<b>config ssh server {maxsession &lt;int 1-8&gt;   contimeout &lt;sec 120-600&gt;   authfail&lt;int 2-20&gt;   rekey [ 10min   30min   60min   never] }(1)</b>
Description	This command allows users to configure the SSH server.

## config ssh server

Parameters	<p><i>maxsession &lt;int 1-8&gt;</i> – Allows the user to set the number of users that may simultaneously access the Switch. The default setting is 8.</p> <p><i>contimeout &lt;sec 120-600&gt;</i> – Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default is 120 seconds.</p> <p><i>authfail &lt;int 2-20&gt;</i> – Allows the administrator to set the maximum number of attempts that a user may try to logon utilizing SSH authentication. After the maximum number of attempts is exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login.</p> <p><i>rekey [10min   30min   60min   never]</i> – Sets the time period that the Switch will change the security shell encryptions.</p>
Restrictions	Only Administrator-level users can issue this command.

Usage example:

To configure the SSH server:

```
DES-1228/ME:4# config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2
```

Success.

```
DES-1228/ME:4#
```

## show ssh server

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

Usage example:

To display the SSH server:

```
DES-1228/ME:4# show ssh server
Command: show ssh server
```

The SSH server configuration

```
max Session           : 8
Connection timeout   : 300
Authfail attempts    : 2
Rekey timeout        : never
port                 : 22
```

```
DES-1228/ME:4#
```

## config ssh user

Purpose	Used to configure the SSH user.
Syntax	<b>config ssh user &lt;username 15&gt; authmode [hostbased [hostname &lt;domain_name 32&gt;] [hostname_IP &lt;domain_name 32&gt; &lt;ipaddr&gt;]   password   publickey]</b>
Description	This command allows users to configure the SSH user authentication method.

## config ssh user

Parameters	<p><i>&lt;username 15&gt;</i> – Enter a username of no more than 15 characters to identify the SSH user.</p> <p><i>authmode</i> – Specifies the authentication mode of the SSH user wishing to log on to the Switch. The administrator may choose between:</p> <p><i>hostbased</i> – This parameter should be chosen if the user wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user.</p> <p><i>hostname &lt;domain_name 32&gt;</i> – Enter an alphanumeric string of up to 32 characters identifying the remote SSH user.</p> <p><i>hostname_IP &lt;domain_name 32&gt; &lt;ipaddr&gt;</i> – Enter the hostname and the corresponding IP address of the SSH user.</p> <p><i>password</i> – This parameter should be chosen to use an administrator defined password for authentication. Upon entry of this command, the Switch will prompt the user for a password, and then to retype the password for confirmation.</p> <p><i>publickey</i> – This parameter should be chosen to use the publickey on a SSH server for authentication.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the SSH user:

```
DES-1228/ME:4# config ssh user Trinity authmode password
```

```
Command: config ssh user Trinity authmode password
```

Success.

```
DES-1228/ME:4#
```

## show ssh user authmode

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

Example usage:

To display the SSH user:

```
DES-1228/ME:4#show ssh user authmode
```

```
Command: show ssh user authmode
```

Current Accounts:

UserName	Authentication	Host	Name	Host	IP
-----	-----	-----	-----		
Trinity	Password				

```
DES-1228/ME:4#
```



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

**config ssh algorithm**

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

Usage example:

To configure SSH algorithm:

```
DES-1228/ME:4# config ssh algorithm Blowfish enable
```

```
Command: config ssh algorithm Blowfish enable
```

```
Success.
```

```
DES-1228/ME:4#
```



**show ssh algorithm**

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

Usage Example:

To display SSH algorithms currently set on the Switch:

```
DES-1228/ME:4#show ssh algorithm
```

```
Command: show ssh algorithm
```

```
Encryption Algorithm
```

```
3DES           :Enabled
```

```
AES128         :Enabled
```

```
AES192         :Enabled
```

```
AES256         :Enabled
```

```
ARC4           :Enabled
```

```
Blowfish       :Enabled
```

```
Cast128        :Enabled
```

```
Twofish128     :Enabled
```

```
Twofish192     :Enabled
```

```
Twofish256     :Enabled
```

```
Data Integrity Algorithm
```

```
MD5            :Enabled
```

```
SHA1           :Enabled
```

```
Public Key Algorithm
```

```
RSA            :Enabled
```

```
DSA            :Enabled
```

```
DES-1228/ME:4#
```

## SMTP COMMANDS

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered using the commands below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events and enhancing security by recording questionable events occurring on the Switch.

The Switch plays four important roles as a client in the functioning of SMTP:

The server and server virtual port must be correctly configured for this function to work properly. This is accomplished in the **config smtp** command by properly configuring the *server* and *server\_port* parameters.

Mail recipients must be configured on the Switch. This information is sent to the server which then processes the information and then e-mails Switch information to these recipients. Up to 8 e-mail recipients can be configured on the Switch using the **config smtp** command by configuring the *add mail\_receiver* and *delete mail\_receiver* parameters.

The administrator can configure the source mail address from which messages are delivered to configured recipients. This can offer more information to the administrator about Switch functions and problems. The personal e-mail can be configured using the **config smtp** command and setting the *self\_mail\_addr* parameter.

The Switch can be configured to send out test mail to first ensure that the recipient will receive e-mails from the SMTP server regarding the Switch. To configure this test mail, the SMTP function must first be enabled using the **enable smtp** command and then by entering the **smtp send\_testmsg** command. All recipients configured for SMTP will receive a sample test message from the SMTP server, ensuring the reliability of this function.

### THE SWITCH WILL SEND OUT E-MAIL TO RECIPIENTS WHEN ONE OR MORE OF THE FOLLOWING EVENTS OCCUR:

When a cold start occurs on the Switch.

When a port enters a link down status.

When a port enters a link up status.

When SNMP authentication has been denied by the Switch.

When a switch configuration entry has been saved to the NVRAM by the Switch.

When an abnormality occurs on TFTP during a firmware download event. This includes *in-process*, *invalid-file*, *violation*, *file-not-found*, *complete* and *time-out* messages from the TFTP server.

When a system reset occurs on the Switch.

Information within the e-mail from the SMTP server regarding switch events includes:

The source device name and IP address.

A timestamp denoting the identity of the SMTP server and the client that sent the message, as well as the time and date of the message received from the Switch. Messages that have been relayed will have timestamps for each relay.

The event that occurred on the Switch, prompting the e-mail message to be sent.

When an event is processed by a user, such as save or firmware upgrade, the IP address, MAC address and User Name of the user completing the task will be sent along with the system message of the event occurred.

When the same event occurs more than once, the second mail message and every repeating mail message following will have the system's error message placed in the subject line of the mail message.

The following details events occurring during the Delivery Process.

Urgent mail will have high priority and be immediately dispatched to recipients while normal mail will be placed in a queue for future transmission.

The maximum number of untransmitted mail messages placed in the queue cannot exceed 30 messages. Any new messages will be discarded if the queue is full.

If the initial message sent to a mail recipient is not delivered, it will be placed in the waiting queue until its place in the queue has been reached, and then another attempt to transmit the message is made.

The maximum attempts for delivering mail to recipients is three. Mail message delivery attempts will be tried every five minutes until the maximum number of attempts is reached. Once reached and the message has not been successfully delivered, the message will be dropped and not received by the mail recipient.

If the Switch shuts down or reboots, mail messages in the waiting queue will be lost.

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

Command	Parameters
enable smtp	
disable smtp	
config smtp	{server <ipaddr>   server_port <tcp_port_number 1-65535>  self_mail_addr <mail_addr 64>  [add mail_receiver <mail_addr 64>   delete mail_receiver <index 1-8>]}(1)
show smtp	
smtp send_testmsg	

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

## enable smtp

Purpose	Used to enable the Switch as a SMTP client.
Syntax	<b>enable smtp</b>
Description	This command, in conjunction with the <b>disable smtp command</b> will enable and disable the Switch as a SMTP client without changing configurations.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SMTP on the Switch.

```
DES-1228/ME:4#enable smtp
```

```
Command: enable smtp
```

```
Success.
```

```
DES-1228/ME:4#
```

## disable smtp

Purpose	Used to disable the Switch as a SMTP client.
Syntax	<b>disable smtp</b>
Description	This command, in conjunction with the <b>enable smtp command</b> will enable and disable the Switch as a SMTP client without changing configurations.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SMTP on the Switch.

```
DES-1228/ME:4#disable smtp
```

```
Command: disable smtp
```

```
Success.
```

```
DES-1228/ME:4#
```

## config smtp

Purpose	Used to configure necessary information in setting up the Switch as an SMTP client.
---------	---

**config smtp**

Syntax	<b>config smtp {server &lt;ipaddr&gt;   server_port &lt;tcp_port_number 1-65535&gt;  self_mail_addr &lt;mail_addr 64&gt; [[add mail_receiver &lt;mail_addr 64&gt;   delete mail_receiver &lt;index 1-8&gt;]](1)</b>
Description	This command will allow the user to set the necessary parameters to configure the SMTP server and mail recipients. This command must be completely configured properly for the SMTP function of the switch to correctly operate.
Parameters	<p><i>server &lt;ipaddr&gt;</i> – Enter the IP address of the SMTP server on a remote device.</p> <p><i>server_port &lt;tcp_port_number 1-65535&gt;</i> – Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is 25.</p> <p><i>self_mail_addr &lt;mail addr 64&gt;</i> – Enter the e-mail address from which mail messages will be sent. This address will be the from address on the e-mail message sent to a recipient. Only one self mail address can be configured for this Switch. This string can be no more than 64 alphanumeric characters.</p> <p><i>add mail_receiver &lt;mail_addr 64&gt;</i> – Choose this parameter to add mail recipients to receive e-mail messages from the Switch. Up to 8 e-mail addresses can be added per Switch.</p> <p><i>delete mail_receiver &lt;index 1-8&gt;</i> – Choose this parameter to delete mail recipients from the configured list receiving e-mail messages from the Switch. Up to 8 e-mail addresses can be added per Switch.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the SMTP settings:

```
DES-1228/ME:4#config smtp server 166.99.66.33 server_port 25 add mail receiver
darren_tremblett@nhl.com
Command: config smtp server 166.99.66.33 server_port 25 add mail receiver
darren_tremblett@nhl.com

Success.

DES-1228/ME:4#
```

**show smtp**

Purpose	Used to view configured parameters for the SMTP function on the Switch.
Syntax	<b>show smtp</b>
Description	This command will display parameters configured for SMTP on the Switch, including server information, mail recipients and the current running status of SMTP on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the SMTP parameters currently configured on the Switch:

```
DES-1228/ME:4#show smtp
Command: show smtp

smtp status: Enabled
smtp server address : 166.99.66.33
smtp server port : 25
self mail address: smtp@1228.dev
```

Index	Mail Receiver Address
-----	-----
1	darren_tremblett@nhl.com
2	dave@yeehaw.com
3	administrator@dlink.com
4	fattony@themob.com
5	
6	
7	
8	

```
DES-1228/ME:4#
```

## smtp send\_testmsg

Purpose	Used to send a test message to mail recipients configured on the Switch.
Syntax	<b>smtp send_testmsg</b>
Description	This command is used to send test messages to all mail recipients configured on the Switch, thus testing the configurations set and the reliability of the SMTP server.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To send a test mail message to all configured mail recipients.

```
DES-1228/ME:4# smtp send_testmsg
Command: smtp send_testmsg
```

```
Subject: This is a SMTP test.
```

```
Content: Hello everybody!!
```

```
Sending mail, please wait...
```

```
Success.
```

```
DES-1228/ME:4#
```

## CABLE DIAGNOSTICS COMMANDS

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

Command	Parameters
<code>cable_diag ports</code>	<code>[&lt;portlist&gt; all]</code>

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

### **cable\_diag ports**

Purpose	Used to test the copper cable. If there is an error on the cable, it can determine the type of error and the position where the error occurred.
Syntax	<b>cable_diag ports [&lt;portlist&gt; all]</b>
Description	For FE port, two pairs of cable will be diagnosed. The type of cable error can be open and short. Open means that the cable in the error pair does not have a connection at the specified position. Short means that the cables in the error pair has a short problem at the specified position. When a port is in link-up status, the test will obtain the distance of the cable. Since the status is link-up, the cable will not have the short or open problem. When a port is in link-down status, the link-down may be caused by many factors. When the port has a normal cable connection, but the remote partner is powered off, the cable diagnosis can still diagnose the health of the cable as if the remote partner is powered on.  When the port does not have any cable connection, the result of the test will indicate no cable. The test will detect the type of error and the position where the error occurs. Note that this test will consume a low number of packets. Since this test is for copper cable, the port with fiber cable will be skipped from the test. Some phy chips can't support Cable Diagnostic function, and it will display at the result.
Parameters	<code>&lt;portlist&gt;</code> – Specifies a range of ports to be tested. <code>all</code> – All ports
Restrictions	None.

Example usage:

To test the cable on specific ports:

```
DES-1228/ME:4#cable_diag ports 1-3,10
```

```
Command: cable_diag ports 1-3,10
```

```
Perform Cable Diagnostics ...
```

Port	Type	Link Status	Test Result	Cable Length (M)
----	-----	-----	-----	-----
1	FE	Link Down	No Cable	-
2	FE	Link Down	No Cable	-
3	FE	Link Up	OK	49
10	FE	Link Down	No Cable	-

```
DES-1228/ME:4#
```

## DHCP LOCAL RELAY COMMANDS

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

Command	Parameters
config dhcp_local _relay	vlan[<vlan_name 32>   vlanid <vidlist>] state [enable   disable]
enable dhcp_local _relay	
disable dhcp _local_relay	
show dhcp _local_relay	

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

### config dhcp\_local\_relay vlan

Purpose	Used to enable/disable DHCP local relay function to vlan.
Syntax	<b>config dhcp_local_relay vlan [&lt;vlan_name 32&gt;  vlanid &lt;vidlist&gt;] state [enable   disable]</b>
Description	The config dhcp_local_relay vlan command is used to enable /disable DHCP local relay function for specified vlan. When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed in broadcast way without change of the source MAC address and gateway address. DHCP option 82 will be automatically added.
Parameters	<vlan_name 32> – The name of the VLAN to be enabled DHCP local relay. <vidlist> – Specifies a range of VLAN IDs to be configured. state – Enable or disable DHCP local relay for specified vlan.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable DHCP local relay for the default vlan:

```
DES-1228/ME:4#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable
```

Success.

```
DES-1228/ME:4#
```

### enable dhcp\_local\_relay

Purpose	Used to enable the DHCP local relay function on the switch.
Syntax	<b>enable dhcp_local_relay</b>
Description	The enable dhcp_local _relay command globally enables the DHCP local relay function on the switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable DHCP local relay function:

```
DES-1228/ME:4#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DES-1228/ME:4#
```

## disable dhcp\_local\_relay

Purpose	Used to disable the DHCP local relay function on the switch.
Syntax	<b>disable dhcp_local_relay</b>
Description	The disable dhcp_local_relay command globally disables the DHCP local relay function on the switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable DHCP local relay function:

```
DES-1228/ME:4#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DES-1228/ME:4#
```

## show dhcp\_local\_relay

Purpose	Used to display the current DHCP local relay configuration.
Syntax	<b>show dhcp_local_relay</b>
Description	The show dhcp_local_relay command displays the current DHCP local relay configuration.
Parameters	None.
Restrictions	None.

Example usage:

To show DHCP local relay function:

```
DES-1228/ME:4# show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status      : Disabled
DHCP/BOOTP Local Relay VLAN List  : 1,3-4

DES-1228/ME:4#
```



## 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	Parameters
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	{ipif <ipif_name 12 >} {trap   log}(1)
disable gratuitous_arp	{ipif <ipif_name 12>} {trap   log}(1)
config gratuitous_arp send periodically ipif	<ipif_name 12> interval <value 0-65535>
show gratuitous_arp	{ipif <ipif_name 12>}

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

### config gratuitous\_arp send ipif\_status\_up

Purpose	Used to enable/disable send gratuitous ARP request while the IP interface status is up.
Syntax	<b>config gratuitous_arp send ipif_status_up [enable   disable]</b>
Description	The command is used to enable/disable sending of gratuitous ARP request packet while 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	<i>enable</i> – Enable sending of gratuitous ARP when IPIF status is up. <i>disable</i> – Disable sending of gratuitous ARP when IPIF status is up.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable a gratuitous ARP request:

```
DES-1228/ME:4#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DES-1228/ME:4#
```

### config gratuitous\_arp send duplicate\_ip\_detected

Purpose	Used to enable/disable the sending of gratuitous ARP requests while duplicate IP addresses are detected
Syntax	<b>config gratuitous_arp send duplicate_ip_detected [enable disable]</b>
Description	The command is used to enable/disable sending of gratuitous ARP request packets while duplicate IPs are detected. By default, the state is enabled. For this command, the duplicate IP detected means that the system has received an ARP request packet that

**config gratuitous\_arp send duplicate\_ip\_detected**

was sent by an IP address that matched the system's own IP address. In this case, the system knows that somebody out there uses an IP address that is conflicting with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.

**Parameters**            *enable* – Enable sending of gratuitous ARP when duplicate IP is detected.  
                              *disable* – Disable sending of gratuitous ARP when duplicate IP is detected.

**Restrictions**            Only Administrator-level users can issue this command.

Example usage:

To enable gratuitous ARP request when a duplicate IP is detected:

```
DES-1228/ME:4#config gratuitous_arp duplicate_ip_detected enable
```

```
Command: config gratuitous_arp duplicate_ip_detected enable
```

```
Success.
```

```
DES-1228/ME:4#
```

**config gratuitous\_arp learning**

**Purpose**                    Used to enable/disable learning of ARP entries in ARP cache based on the received gratuitous ARP packets.

**Syntax**                    **config gratuitous\_arp 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 command is used to enable/disable learning of ARP entry 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 the gratuitous ARP learning, the system will not learn new entry 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 learning of ARP entries based on the received gratuitous ARP packet.  
                              *disable* – Disable learning of ARP entry based on the received gratuitous ARP packet.

**Restrictions**            Only Administrator-level users can issue this command.

Example usage:

To enable learning of ARP entries based on the received gratuitous ARP packets:

```
DES-1228/ME:4# config gratuitous_arp learning enable
```

```
Command: config gratuitous_arp learning enable
```

```
Success.
```

```
DES-1228/ME:4#
```

**config gratuitous\_arp periodical\_send**

**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 <value 0-65535>**

**Description**             This command is used to configure the interval for periodical sending of gratuitous ARP request packets. By default, the interval is 0.

**Parameters**            <ipif\_name 12> – Interface name of L3 interface.

**config gratuitous\_arp periodical\_send**

*<value 0-65535>* – Periodically send gratuitous ARP interval time in seconds. 0- means it will not send gratuitous ARP periodically.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure gratuitous ARP intervals for the IPIF System:

```
DES-1228/ME:4#config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DES-1228/ME:4#
```

**enable gratuitous\_arp trap and log**

Purpose Used to enable the gratuitous ARP trap and log.

Syntax **enable gratuitous\_arp {ipif <ipif\_name 12 >} {trap | log}(1)**

Description The command is used to enable gratuitous ARP trap and log states. The switch can trap and log the IP conflict event to inform the administrator. By default, the trap is disabled and event log is enabled.

Parameters *<ipif\_name 12>* – Interface name of L3 interface.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To enable the System's interface gratuitous ARP log and trap:

```
DES-1228/ME:4#enable gratuitous_arp System trap log
Command: enable gratuitous_arp System trap log

Success.

DES-1228/ME:4#
```

**disable gratuitous\_arp trap and log**

Purpose Used to disable the gratuitous ARP trap and log.

Syntax **disable gratuitous\_arp {ipif <ipif\_name 12>} {trap | log}(1)**

Description The command is used to disable the gratuitous ARP trap and log states. The switch can trap and log the IP conflict event to inform the administrator. By default, the trap is disabled and event log is enabled.

Parameters *<ipif\_name 12>* – Interface name of L3 interface.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To disable the System's interface gratuitous ARP log and trap:

```
DES-1228/ME:4#disable gratuitous_arp System trap log
Command: disable gratuitous_arp System trap log

Success.

DES-1228/ME:4#
```

## show gratuitous\_arp

Purpose	Used to display gratuitous ARP configuration.
Syntax	<b>show gratuitous_arp {ipif &lt;ipif_name&gt;}</b>
Description	The show gratuitous_arp command is used to display gratuitous ARP configurations.
Parameters	<ipif_name 12> – Interface name of L3 interface.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display gratuitous ARP log and trap states:

```
DES-1228/ME:4# show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF status up           : Enabled
Send on Duplicate_IP_Detected    : Disabled
Gratuitous ARP Learning          : Enabled

IP Interface Name : System
Gratuitous ARP Trap/Log          : Disabled
Gratuitous ARP Log               : Enabled
Gratuitous ARP Periodical Send Interval : 5

DES-1228/ME:4#
```

## VLAN TRUNKING COMMANDS

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

Command	Parameters
enable vlan_trunk	
disable vlan_trunk	
config vlan_trunk ports	[<portlist> all] state [enable disable]
show vlan_trunk	

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

### enable vlan\_trunk

Purpose	Used to enable the VLAN trunk function.
Syntax	<b>enable vlan_trunk</b>
Description	When the VLAN trunk function is enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the VLAN Trunk:

```
DES-1228/ME:4#enable vlan_trunk
Command: enable vlan_trunk

Success.

DES-1228/ME:4#
```

### disable vlan\_trunk

Purpose	Used to disable the VLAN trunk function.
Syntax	<b>disable vlan_trunk</b>
Description	This command is used to disable the VLAN trunk function.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the VLAN Trunk:

```
DES-1228/ME:4#disable vlan_trunk
Command: disable vlan_trunk

Success.

DES-1228/ME:4#
```

**config vlan\_trunk**

Purpose	Used to configure a port as a VLAN trunk port.
Syntax	<b>config vlan_trunk ports [&lt;portlist&gt; all]   state [enable disable]</b>
Description	<p>This command is used to configure a port as a VLAN trunk port. By default, none of the ports on the Switch are VLAN trunk ports. A VLAN trunk port and a non-VLAN trunk port cannot be grouped as an aggregated link. To change the VLAN trunk setting for an aggregated link, the user must apply the command to the master port. However, this setting will disappear as the aggregated link is destroyed, and the VLAN trunk setting of the individual port will follow the original setting of the port.</p> <p>If the command is applied to link aggregation member port excluding the master, the command will be rejected.</p> <p>The ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as VLAN trunk ports, they are allowed to form an aggregated link.</p> <p>For a VLAN trunk port, the VLANs on which the packets can be by passed will not be advertised by GVRP on that particular port. However, since the traffic on these VLANs are forwarded, this vlan trunk port should participate the MSTP instances corresponding to these VLAN.</p>
Parameters	<p><i>&lt;portlist&gt;</i> – Specifies the list of ports to be configured.</p> <p><i>enable</i> – Specifies that the port is a VLAN trunk port.</p> <p><i>disable</i> – Specifies that the port is not a VLAN trunk port.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a VLAN Trunk port:

```
DES-1228/ME:4#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DES-1228/ME:4#
```

To configure a VLAN Trunk port if Port 6 is LA-1 member port; port 7 is LA-2 master port.

```
DES-1228/ME:4# config vlan_trunk ports 6-7 state enable
```

```
Command: config vlan_trunk ports 6-7 state enable
```

Can not operate the member ports of any trunk.

```
DES-1228/ME:4# config vlan_trunk ports 7 state disable
```

```
Command: config vlan_trunk ports 7 state disable
```

Success.

```
DES-1228/ME:4# config vlan_trunk ports 6-7 state disable
```

```
Command: config vlan_trunk ports 6-7 state disable
```

Can not operate the member ports of any trunk.

```
DES-1228/ME:4#
```

To configure a VLAN Trunk port if Port 6 is LA-1 member port, port 7 is LA-1 master port.

```
DES-1228/ME:4# config vlan_trunk ports 6-7 state enable
```

```
Command: config vlan_trunk ports 6-7 state enable
```

Success.

```
DES-1228/ME:4#
```

To configure a VLAN Trunk port if Port 6,7 have the same VLAN configurations before enable VLAN trunking. Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DES-1228/ME:4# config vlan_trunk ports 7 state disable
```

```
Command: config vlan_trunk ports 7 state disable
```

Success.

```
DES-1228/ME:4# config vlan_trunk ports 6-7 state disable
```

```
Command: config vlan_trunk ports 6-7 state disable
```

Success.

```
DES-1228/ME:4#
```

## show vlan\_trunk

Purpose	Used to display VLAN trunk configuration.
Syntax	<b>show vlan_trunk</b>
Description	Shows the VLAN trunk information.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display VLAN Trunk information:

```
DES-1228/ME:4#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk           :Enable
VLAN Trunk Port      :1-5,7

DES-1228/ME:4#
```



## ASYMMETRIC VLAN COMMANDS

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

Command	Parameters
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	

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

### enable asymmetric\_vlan

Purpose	Used to enable the asymmetric VLAN function on the Switch.
Syntax	<b>enable asymmetric_vlan</b>
Description	This command enables the asymmetric VLAN function on the Switch
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable asymmetric VLANs:

```
DES-1228/ME:4#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DES-1228/ME:4#
```

### disable asymmetric\_vlan

Purpose	Used to disable the asymmetric VLAN function on the Switch.
Syntax	<b>disable asymmetric_vlan</b>
Description	This command disables the asymmetric VLAN function on the Switch
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable asymmetric VLANs:

```
DES-1228/ME:4#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DES-1228/ME:4#
```

## show asymmetric\_vlan

Purpose	Used to view the asymmetric VLAN state on the Switch.
Syntax	<b>show asymmetric_vlan</b>
Description	This command displays the asymmetric VLAN state on the Switch
Parameters	None.
Restrictions	None.

Example usage:

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

```
DES-1228/ME:4#show asymmetric_vlan
```

```
Command: show asymmetric_vlan
```

```
Asymmetric VLAN: Enabled
```

```
DES-1228/ME:4#
```

## IGMP SNOOPING MULTICAST VLAN COMMANDS

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

Command	Parameters
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 32> {[add  delete] [member_port <portlist>   tag_member_port <portlist>  source_port <portlist>]}state [enable   disable]]replace_source_ip [<ipaddr> none]}(1)
config igmp_snooping multicast_vlan_group	<vlan_name 32> [ add <mcast_address_list>   delete [<mcast_address_list>   all]]
show igmp_snooping multicast_vlan_group	{< vlan_name 32> }
delete igmp_snooping multicat_vlan	<vlan_name 32>
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
show igmp_snooping multicast_vlan	{<vlan_name 32>}

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

### create igmp\_snooping multicast\_vlan

Purpose	Used to create a multicast VLAN
Syntax	<b>create igmp_snooping multicast_vlan &lt;vlan_name 32&gt; &lt;vlanid 2-4094&gt;</b>
Description	<p>The create igmp_snooping multicast_vlan command will create a multicast_vlan. Multiple multicast VLAN can be configured.</p> <p>The ISM VLAN being created can not exist in the 1Q VLAN database. Multiple ISM VLAN can be created. The ISM VLAN snooping function co-exist with the 1Q VLAN snooping function.</p>
Parameters	<p>&lt;vlan_name&gt; – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.</p> <p>&lt;vlanid&gt; – The VLAN ID of the multicast VLAN to be create. The range is 2-4094</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create IGMP snoop multicast VLAN mv12:

```
DES-1228/ME:4# create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2

Success.

DES-1228/ME:4#
```

## config igmp\_snooping multicast\_vlan

Purpose	Used to configure the parameter of the specific multicast VLAN.
Syntax	<b>config igmp_snooping multicast_vlan &lt;vlan_name 32&gt; {[add  delete] [member_port &lt;portlist&gt;   tag_member_port &lt;portlist&gt;  source_port &lt;portlist&gt;]}state [enable   disable]]replace_source_ip [&lt;ipaddr&gt; none]}(1)</b>
Description	<p>The <b>config igmp_snooping multicast_vlan</b> command allows you to add a member port, add a tag member port, and add a source port to the port list. The member port will automatically become the untagged member of the multicast VLAN, the tag member port and the source port will automatically become the tagged member of the multicast VLAN. To change the port list, the new port list will replace the previous port list if the add or delete is not specified.</p> <p>The member port list and source port list can not overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN.</p> <p>The multicast VLAN must be created first before configuration.</p>
Parameters	<p><i>&lt;vlan_name&gt;</i> – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.</p> <p><i>member_port &lt;portlist&gt;</i> – A range of member ports to add to the multicast VLAN. They will become the untagged member port of the ISM VLAN.</p> <p><i>tag_member_port &lt;portlist&gt;</i> – Specifies the tagged member port of the ISM VLAN.</p> <p><i>source_port</i> – A range of source ports to add to the multicast VLAN.</p> <p><i>state</i> - enable or disable multicast VLAN for the chosen VLAN.</p> <p><i>replace_source_ip</i> – With the IGMP snooping function, the IGMP 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 IP address. If none is specified the source IP address will not be replaced.</p> <p><i>none</i> – Specifies that the source IP address will not be replaced.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure an IGMP snoop multicast VLAN:

```
DES-1228/ME:4# config igmp_snooping multicast_vlan v1 add member_port 1,3 state enable
Command: config igmp_snooping multicast_vlan v1 add member_port 1,3 state enable


Success.

DES-1228/ME:4#
```

## config igmp\_snooping multicast\_vlan\_group

Purpose	Used to configure the multicast group which will be learned with the specific multicast VLAN.
---------	---

**config igmp\_snooping multicast\_vlan\_group**

Syntax	<b>&lt;vlan_name 32&gt; [ add &lt;mcast_address_list&gt;   delete [&lt;mcast_address_list&gt;   all]]</b>
Description	Used to configure the multicast group which will be learned with the specific multicast VLAN. There are two cases need to be considered. The join packet will be learned with the multicast VLAN that contain the destination multicast group. If the destination multicast group of the join packet can not be classified into any multicast VLAN that this port belong, then the join packet will be learned with the natural VLAN of the packet.
	 <b>Note:</b> The same multicast group can not be overlapped in different multicast VLANs. Multiple multicast groups can be added to a multicast VLAN.
Parameters	<p><b>&lt;vlan_name 32&gt;</b> – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters.</p> <p><b>&lt;mcast_address_list&gt;</b> – The list of multicast groups that will be learned with the specified multicast VLAN.</p> <p><b>all</b> – All multicast groups will be selected from the specified multicast VLAN.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a group to a multicast VLAN:

```
DES-1228/ME:4#config igmp_snooping multicast_vlan_group v1 add 225.1.1.1
Command: config igmp_snooping multicast_vlan_group v1 add 225.1.1.1
```

Success.

```
DES-1228/ME:4#
```

**show igmp\_snooping multicast\_vlan\_group**

Purpose	Used to display the multicast groups configured for the specified multicast VLAN.
Syntax	<b>show igmp_snooping multicast_vlan_group {&lt; vlan_name 32&gt; }</b>
Description	Used to display the multicast groups configured for the specified multicast VLAN.
Parameters	<b>&lt;vlan_name 32&gt;</b> – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters.
Restrictions	None.

Example usage:

To display the multicast groups configured for a multicast VLAN.

```
DES-1228/ME:4#show multicast_vlan_group v1
Command: show multicast_vlan_group v1
```

VLAN Name	VLAN ID	From	To
v1	100	224.19.62.34	224.19.162.200

```
DES-1228/ME:4#
```

**delete igmp\_snooping multicast\_vlan**

**delete igmp\_snooping multicast\_vlan**

Purpose	Used to delete a multicast VLAN.
Syntax	<b>delete igmp_snooping multicast_vlan &lt;vlan_name 32&gt;</b>
Description	The delete igmp_snooping multicast_vlan command allows you to delete multicast_vlan.
Parameters	<vlan_name 32> – The name of the multicast VLAN to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an IGMP snoop multicast VLAN:

```
DES-1228/ME:4# delete igmp_snooping multicat_vlan v1
Command: delete igmp_snooping multicat_vlan v1
```

Success.

```
DES-1228/ME:4#
```

**enable igmp\_snooping multicast\_vlan**

Purpose	Used to enable the multicast VLAN function.
Syntax	<b>enable igmp_snooping multicast_vlan</b>
Description	This command controls the multicast VLAN function. The ISM VLAN will take effect when igmp snooping multicast_vlan is enabled. By default, the multicast VLAN is in a disabled state.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable IGMP snoop multicast VLAN:

```
DES-1228/ME:4# enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan
```

Success.

```
DES-1228/ME:4#
```

**disable igmp\_snooping multicast\_vlan**

Purpose	Used to disable the multicast VLAN function.
Syntax	<b>disable igmp_snooping multicast_vlan</b>
Description	This command controls the multicast VLAN function. The ISM VLAN will take effect when igmp snooping multicast vlan is enabled. By default, the multicast VLAN is in a disabled state.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable IGMP snoop multicast VLAN:

```
DES-1228/ME:4#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DES-1228/ME:4#
```

**show igmp\_snooping multicast\_vlan**

Purpose	Used to show the information of multicast VLAN.
Syntax	<b>show igmp_snooping multicast_vlan {&lt;vlan_name 32&gt;}</b>
Description	The <b>show igmp_snooping multicast_vlan</b> command allows you to show the information of multicast VLAN.
Parameters	<vlan_name 32> – The name of the multicast VLAN to be shown.
Restrictions	None.

Example usage:

To display IGMP snoop multicast VLAN:

```
DES-1228/ME:4#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

Muticast Vlan Global State : Enabled

VID                : 123      VLAN Name: 123
Member Ports       :
Tagged Member Ports :
Source Ports       :
Status             : Disabled
Replace Source IP  : None

DES-1228/ME:4#
```

## LLDP COMMANDS

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

Command	Parameters
enable lldp	
disable lldp	
config lldp message_tx_interval	<sec 5 - 32768 >
config lldp message_tx_hold_multiplier	< int 2 - 10 >
config lldp tx_delay	< sec 1 - 8192 >
config lldp reinit_delay	< sec 1 - 10 >
config lldp notification_interval	<sec 5 - 3600 >
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> [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] dot1_tlv_pvid [enable   disable]
config lldp ports	[<portlist> all] dot1_tlv_vlan_name [vlan [all   <vlan_name 32> ]   vlanid <vidlist> ] [enable   disable]
config lldp ports	[<portlist> all] dot1_tlv_protocol_identity[all   { eapol   lacp   gvrp   stp }] [enable   disable]
config lldp ports	config lldp ports [<portlist> all] dot3_tlvs [all   {mac_phy_configuration_status   link aggregation   power_via_mdi   maximum_frame_size}] [enable   disable]
config lldp forward_message	[enable   disable]
show lldp	
show lldp mgt_addr	{ipv4 <ipaddr>}
show lldp ports	{<portlist>}
show lldp local_ports	{ <portlist> } {mode [brief   normal   detailed]}
show lldp remote_ports	{<portlist>} {mode [brief   normal   detailed]}
show lldp statistics	
show lldp statistics ports	{<portlist>}

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

### enable lldp

Purpose	Used to enable LLDP operations on the switch.
Syntax	<b>enable lldp</b>
Description	This is a global control for the LLDP function. When this function is enabled, the switch can start to transmit LLDP packets and receive



**enable lldp**

and process the LLDP packets.

The specific function of each port will depend on the per port LLDP setting. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table.

The default state for LLDP is disabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example usage

To enable LLDP:

```
DES-1228/ME:4# enable lldp
```

```
Command: enable lldp
```

```
Success.
```

```
DES-1228/ME:4#
```

**disable lldp**

Purpose

Used to disable LLDP operation on the switch.

Syntax

**disable lldp**

Description

The switch will stop sending and receiving of LLDP advertisement packets.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example usage

To disable LLDP:

```
DES-1228/ME:4# disable lldp
```

```
Command: disable lldp
```

```
Success.
```

```
DES-1228/ME:4#
```

**config lldp message\_tx\_interval**

Purpose

Used to change the packet transmission interval.

Syntax

**config lldp message\_tx\_interval <sec 5 - 32768 >**

Description

This interval controls how often active ports retransmit advertisements to their neighbors.

Parameters

*message\_tx\_interval* – Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The range is from 5 to 32768 seconds. The default setting is 30 seconds.

Restrictions

Only Administrator-level users can issue this command.

## Example usage

To change the packet transmission interval:

```
DES-1228/ME:4# config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DES-1228/ME:4#
```

### config lldp message\_tx\_hold\_multiplier

Purpose	This command is used to configure the message hold multiplier.
Syntax	<b>config lldp message_tx_hold_multiplier &lt; int 2 - 10 &gt;</b>
Description	This parameter is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU. TheTTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message_tx_interval * message_tx_hold_multiplier). At the partner switch, when the time-to-Live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.
Parameters	<i>message_tx_hold_multiplier</i> – The range is from 2 to 10. The default setting 4.
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To change the multiplier value:

```
DES-1228/ME:4# config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

DES-1228/ME:4#
```

### config lldp tx\_delay

Purpose	Used to change the minimum time (delay-interval) of any LLDP port. It will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The tx_delay defines the minimum interval between the sending of LLDP messages due to constant changes of MIB content.
Syntax	<b>config lldp tx_delay &lt; sec 1–8192 &gt;</b>
Description	The LLDP message_tx_interval (transmit interval) must be greater than or equal to (4 x tx_delay interval).
Parameters	<i>tx_delay</i> – The range is from 1 second to 8192 seconds. The default setting 2 seconds. NOTE: txDelay should be less than or equal to 0.25 * msgTxInterval
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To configure the delay-interval interval:

```
DES-1228/ME:4# config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DES-1228/ME:4#
```

**config lldp reinit\_delay**

Purpose	Change the minimum time of reinitialization delay interval.
Syntax	<b>config lldp reinit_delay &lt; sec 1 – 10 &gt;</b>
Description	An re-enabled LLDP port will wait for reinit_delay after last disable command before reinitializing
Parameters	reinit_delay – The range is from 1 second to 10 seconds. The default setting 2 seconds.
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To change the re-initialization delay interval:

```
DES-1228/ME:4# config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DES-1228/ME:4#
```

**config lldp notification\_interval**

Purpose	Used to configure the timer of the notification interval used to send notifications to configured SNMP trap receiver(s).
Syntax	<b>config lldp notification_interval &lt;sec 5 - 3600 &gt;</b>
Description	Globally change the interval between successive LLDP change notifications generated by the switch.
Parameters	<i>notification_interval</i> – The range is from 5 second to 3600 seconds. The default setting is 5 seconds.
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To change the notification interval:

```
DES-1228/ME:4# config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DES-1228/ME:4#
```

**config lldp ports notification**

Purpose	Used to configure each port for sending notifications to configured SNMP trap receiver(s).
---------	--

## config lldp ports notification

Syntax	<b>config lldp ports</b> [<portlist> all] notification [enable   disable]
Description	Enable or disable each port for sending change notifications to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout and information update. And the changed type includes any data update /insert/remove.
Parameters	<portlist> – Specified a range of ports to be configured. all – To set all ports in the system, you may use the “all” parameter. notification – Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.
Restrictions	Only Administrator-level users can issue this command.

### Example usage

To change the port SNMP notification state:

```
DES-1228/ME:4# config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DES-1228/ME:4#
```

## config lldp admin\_status

Purpose	Used to configure per-port transmit and receive modes.
Syntax	<b>config lldp ports</b> [<portlist> all] admin_status [tx_only   rx_only   tx_and_rx   disable]
Description	These options enable the Switch to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.
Parameters	<portlist> – Specified a range of ports to be configured. all – To set all ports in the system, you may use the “all” parameter. admin_status – To set the admin status. <b>tx_only</b> : Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices. <b>rx_only</b> : Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors. <b>tx_and_rx</b> : Configure the specified port(s) to both transmit and receive LLDP packets. <b>disable</b> : Disable LLDP packet transmit and receive on the specified port(s). The default per port state is tx_and_rx.
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To configure the port's transmit and receive mode:

```
DES-1228/ME:4# config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DES-1228/ME:4#
```

**config mgt\_addr**

Purpose	Used to enable or disable the port(s) which have been specified for advertising the indicated management address instances.
Syntax	<b>config lldp ports [&lt;portlist&gt; all] mgt_addr ipv4 &lt;ipaddr&gt; [enable   disable]</b>
Description	This command specifies whether the system's IP address needs to be advertised from the specified port. For layer 3 devices, each managed address can be individually specified. The management addresses that are added in the list will be advertised in the LLDP from the specified interface associated with each management address. The interface for that management address will be also advertised in the if-index form.
Parameters	<p>&lt;portlist&gt; – Specified a range of ports to be configured.</p> <p>all – To set all ports in the system, you may use the “all” parameter.</p> <p>ipv4 – IP address of IPV4.</p>
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To enable port 1 to port 2 for manage address entries:

```
DES-1228/ME:4# config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable

Success

DES-1228/ME:4#
```

**config lldp basic\_tlvs**

Purpose	Used to configure an individual port or group of ports to exclude one or more of the optional TLV data types from outbound LLDP advertisements.
Syntax	<b>config lldp ports [&lt;portlist&gt; all] basic_tlvs [all   {port_description   system_name   system_description   system_capabilities}] [enable   disable]</b>
Description	An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, Time to Live TLV). The mandatory type can not be disabled. There are also four data types which can be optionally selected. They are port_description, system_name, system_description, and system_capability.
Parameters	<p>&lt;portlist&gt; – Specified a range of ports to be configured.</p> <p>all – To set all ports in the system, you may use the “all” parameter.</p> <p>port_description – This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled.</p> <p>system_name – This TLV optional data type indicates that the LLDP agent should transmit</p>

## config lldp basic\_tlvs

'System Name TLV'. The default state is disabled.

*system\_description* – This TLV optional data type indicates that the LLDP agent should transmit 'System Description TLV'. The default state is disabled.

*system\_capabilities* – This TLV optional data type indicates that the LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router functions, and whether the provided functions are currently enabled. The default state is disabled.

Restrictions Only Administrator-level users can issue this command.

### Example usage

To configure the Switch to exclude the system name TLV from outbound LLDP advertisements on all ports:

```
DES-1228/ME:4# config lldp ports all basic_tlvs system_name enable
```

```
Command: config lldp ports all basic_tlvs system_name enable
```

```
Success.
```

```
DES-1228/ME:4#
```

## config lldp dot1\_tlv\_pvid

Purpose Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port vlan ID TLV data types from outbound LLDP advertisements.

Syntax **config lldp ports [<portlist>|all] dot1\_tlv\_pvid [enable | disable]**

Description This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port.

Parameters <portlist> – Specified a range of ports to be configured.

*all* – To set all ports in the system, you may use the “all” parameter.

*dot1\_tlv\_pvid* – This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disable.

Restrictions Only Administrator-level users can issue this command.

### Example usage

To configure the vlan name TLV from the outbound LLDP advertisements for all ports:

```
DES-1228/ME:4# config lldp ports all dot1_tlv_pvid enable
```

```
Command: config lldp ports all dot1_tlv_pvid enable
```

```
Success.
```

```
DES-1228/ME:4#
```

## config lldp dot1\_tlv\_vlan\_name

Purpose Used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 Organizational VLAN name TLV data types from outbound LLDP advertisements.

Syntax **config lldp ports [<portlist>|all] dot1\_tlv\_vlan\_name [vlan [all | <vlan\_name 32> ] | vlandid <vidlist> ] [enable | disable]**

Description This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs those enabled VLAN IDs will be advertised.

**config lldp dot1\_tlv\_vlan\_name**

Parameters	<p><i>&lt;portlist&gt;</i> – Specified a range of ports to be configured.</p> <p><i>all</i> – To set all ports in the system, you may use the “all” parameter.</p> <p><i>dot1_tlv_vlan_name</i> – This TLV optional data type indicates whether the corresponding Local System’s VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs those enabled VLAN IDs will be advertised. The default state is disable.</p>
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To configure the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DES-1228/ME:4# config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
```

```
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
```

Success.

```
DES-1228/ME:4#
```

**config lldp dot1\_tlv\_protocol\_identity**

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 organization protocol identity TLV data types from outbound LLDP advertisements.
Syntax	<b>config lldp ports [<i>&lt;portlist&gt;</i>][all] dot1_tlv_protocol_identity [all   {<i>eapol</i>   <i>lACP</i>   <i>gvrp</i>   <i>stp</i> }][enable   disable]</b>
Description	This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations which are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.
Parameters	<p><i>&lt;portlist&gt;</i> – Specified a range of ports to be configured.</p> <p><i>all</i> – To set all ports in the system, you may use the “all” parameter.</p> <p><i>dot1_tlv_protocol_identity</i> – This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised. The default state is disable.</p>
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To configure the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DES-1228/ME:4# config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DES-1228/ME:4#
```

## config lldp dot3\_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.3 organization specific TLV data types from outbound LLDP advertisements.
Syntax	<b>config lldp ports [&lt;portlist&gt; all] dot3_tlvs [all   {mac_phy_configuration_status   link aggregation   power_via_mdi   maximum_frame_size}] [enable   disable]</b>
Description	Each Specific TLV in this extension can be enabled individually.
Parameters	<p><i>&lt;portlist&gt;</i> – Specified a range of ports to be configured.</p> <p><i>all</i> – To set all ports in the system, you may use the “all” parameter.</p> <p><i>mac_phy_configuration_status</i> – This TLV optional data type indicates that LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port support the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disable.</p> <p><i>link_aggregation</i> – This TLV optional data type indicates that LLDP agent should transmit 'Link Aggregation TLV'. This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in a aggregated link, and the aggregated port ID. The default state is disable.</p> <p><i>maximum_frame_size</i> – This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV'. The default state is disable .</p>
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To configure the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DES-1228/ME:4#config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

DES-1228/ME:4#
```

## config lldp forward\_message

Purpose	Used to configure forwarding of lldpdu packet when LLDP is disabled.
Syntax	<b>config lldp forward_message [enable   disable]</b>
Description	When lldp is disabled and lldp forward_message is enabled, the received LLDPDU packet will be forwarded. The default state is disable.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.



## Example usage

To configure the LLDP forward\_llpdu:

```
DES-1228/ME:4# config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DES-1228/ME:4#
```

**show lldp**

Purpose	This command displays the switch's general LLDP configuration status.
Syntax	<b>show lldp</b>
Description	This command displays the switch's general LLDP configuration status.
Parameters	None.
Restrictions	None.

## Example usage

To display the LLDP system level configuration status:

```
DES-1228/ME:4# show lldp
Command: show lldp

LLDP system information
  Chassis Id Subtype      : MACADDRESS
  Chassis Id              : 00-15-E9-41-5A-A7
  System Name             : D-Link
  System Description      : Metro Ethernet Switch
  System Capabilities     : Repeater, Bridge,

LLDP Configurations
  LLDP Status             : Disable
  LLDP Forward Status     : Disable
  Message Tx Interval     : 30
  Message Tx Hold Multiplier: 4
  ReInit delay            : 2
  Tx Delay                : 2
  Notification Interval   : 5

DES-1228/ME:4#
```

**show lldp mgt\_addr**

Purpose	Used to display the lldp management address information.
Syntax	<b>show lldp mgt_addr {ipv4 &lt;ipaddr&gt;}</b>
Description	Displays the lldp management address information.
Parameters	<i>ipv4</i> – IP address of IPV4.
Restrictions	None.

## Example usage

To display the management address information:

```
DES-1228/ME:4#show lldp mgt_addr ipv4 192.168.69.123
Command: show lldp mgt_addr ipv4 192.168.69.123

Address 1 :
-----
Subtype           : IPv4
Address           : 192.168.69.123
IF Type          : Unknown
OID              : 1.3.6.1.4.1.171.11.116.1
Advertising Ports :

DES-1228/ME:4#
```

## show lldp ports

Purpose	Display the LLDP per port configuration for advertisement options.
Syntax	<b>show lldp ports {&lt;portlist&gt; }</b>
Description	This command displays the LLDP per port configuration for advertisement options.
Parameters	<portlist> – Specifies a range of ports to be displayed. When port list is not specified, information for all ports will be displayed.
Restrictions	None.

## Example usage

To display the LLDP per port TLV option configuration:

```
DES-1228/ME:4# show lldp ports 1
Command: 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 VLAN Name     (NONE.)
  Enabled protocol_identity
    (NONE.)
  MAC/PHY Configuration/Status Disable
  Link Aggregation      Disable
  Maximum Frame Size    Disable

DES-1228/ME:4#
```

## show lldp local\_ports

Purpose	Used to display the per-port information currently available for populating outbound LLDP advertisements.
Syntax	<b>show lldp local_ports {&lt;portlist&gt;} {mode [brief   normal   detailed]}</b>
Description	This command displays the per-port information currently available for populating outbound LLDP advertisements.
Parameters	<p><i>&lt;portlist&gt;</i> – Specified a range of ports to be configured. When a port list is not specified, information for all ports will be displayed.</p> <p><i>brief</i> – Display the information in brief mode.</p> <p><i>normal</i> – Display the information in normal mode. This is the default display mode.</p> <p><i>detailed</i> – Display the information in detailed mode.</p>
Restrictions	None.

## Example usage

To display outbound LLDP advertisements for individual ports in detail:

```
DES-1228/ME:4# show lldp local_ports 1 mode detailed
Command: show lldp local_ports 1 mode detailed

Port ID : 1
-----
Port Id Subtype           : Local
Port Id                   : 1/1
Port Description          : D-Link DES-1228/ME R1.00 Port 1
Port PVID                 : 1
Management Address Count : 1
    Subtype               : IPv4
    Address                : 192.168.69.123
    IF Type                : Unknown
    OID                    : 1.3.6.1.4.1.171.11.116.1
PPVID Entries Count      : 0
(NONE)
VLAN Name Entries Count  : 1
    Entry 1 :
        Vlan ID           : 1
        Vlan Name         : default
Protocol Identity Entries Count : 0
(NONE)
MAC/PHY Configuration/Status :
    Auto-negotiation Support : Supported
    Auto-negotiation Enabled : Enabled
    Auto-negotiation Advertised Capability : 0005(hex)
    Auto-negotiation Operational MAU Type : 0010(hex)
Power Via MDI            : Not Supported
Link Aggregation         :
    Aggregation Capability   : Aggregated
    Aggregation Status      : Not Currently In Aggregation
    Aggregation Port ID     : 0
Maximum Frame Size       : 1536
DES-1228/ME:4#
```

To display outbound LLDP advertisements for specific ports in normal mode:

```
DES-1228/ME:4#show lldp local_ports 1 mode normal
Command: show lldp local_ports 1 mode normal

Port ID : 1
-----
Port Id Subtype           : Local
Port Id                   : 1/1
Port Description          : D-Link DES-1228/ME R1.00 Port 1
Port PVID                 : 1
Management Address Count : 1
PPVID Entries Count      : 0
VLAN Name Entries Count  : 1
Protocol Identity Entries Count : 0
MAC/PHY Configuration/Status : (See detail)
Power Via MDI             : (See detail)
Link Aggregation         : (See detail)
Maximum Frame Size       : 1536

DES-1228/ME:4#
```

To display outbound LLDP advertisements for specific ports in brief mode:

```
DES-1228/ME:4#show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief

Port ID : 1
-----
Port Id Subtype           : Local
Port Id                   : 1/1
Port Description          : D-Link DES-1228/ME R1.00 Port 1

DES-1228/ME:4#
```

## show lldp remote\_ports

Purpose	Used to display the information learned from the neighbor.
Syntax	<b>show lldp remote_ports</b> {<portlist>} {mode [brief   normal   detailed]}
Description	This command displays information learnt from the neighbor parameters. Due to the memory limitations, the switch can only receive 32 VLAN Name entries and 10 Management Address entries.
Parameters	<i>&lt;portlist&gt;</i> – Specified a range of ports to be configured. When a port list is not specified, information for all ports will be displayed. <i>brief</i> – Display the information in brief mode. <i>normal</i> – Display the information in normal mode. This is the default display mode. <i>detailed</i> – Display the information in detailed mode.
Restrictions	None.

## Example usage

To display remote table entries in brief mode:

```
DES-1228/ME:4# show lldp remote_ports 1-2 mode brief
Command: show lldp remote_ports 1-2 mode brief

Port ID: 1
-----
Remote Entities Count : 2
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-01
  Port ID Subtype        : Local
  Port ID                 : 1/3
  Port Description       : D-Link DES-1228/ME R1.00 Port 3

Entity 2
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-02
  Port ID Subtype        : Local
  Port ID                 : 1/4
  Port Description       : D-Link DES-1228/ME R1.00 Port 4

DES-1228/ME:4#
```

To display remote table entries in normal mode:

```
DES-1228/ME:4# show lldp remote_ports ports 1 mode normal
Command: show lldp remote_ports ports 1 mode normal

Port ID : 1
-----
Remote Entities Count : 1
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-01
  Port ID Subtype        : Local
  Port ID                 : 1/3
  Port Description        : D-Link DES-1228/ME R1.00 Port 3
  System Name             : Switch1
  System Description      :
  System Capabilities     : Repeater, Bridge
  Management Address Count : 1
  Port VLAN ID            : 1
  PPVID Entries Count     : 5
  VLAN Name Entries Count : 3
  Protocol Id Entries Count : 2
  MAC/PHY Configuration Status : (See Detail)
  Power Via MDI            : (See Detail)
  Link Aggregation        : (See Detail)
  Maximum Frame Size      : 1536
  Unknown TLVs Count      : 2

DES-1228/ME:4#
```

To display remote table entries in detailed mode:

```

DES-1228/ME:4# show lldp remote_ports 1 mode detailed
Command: show lldp remote_ports 1 mode detailed

Port ID : 1
-----
Remote Entities count : 1
Entity 1
  Chassis Id Subtype      : MACADDRESS
  Chassis Id              : 00-00-00-48-46-29
  Port Id Subtype         : LOCAL
  Port ID                 : 1/16
  Port Description        : D-Link DES-1228/ME R1.00 Port 16
  System Name             :
  System Description      : Metro Ethernet Switch
  System Capabilities     : Repeater, Bridge,
  Management Address count : 1
    Entry 1 :
      Subtype      : IPv4
      Address      : 10.48.46.128
      IF Type      : unknown
      OID          : 1.3.6.1.4.1.171.11.116.1

  Port PVID              : 1
  PPVID Entries count   : 0
    (None.)

  VLAN Name Entries count : 1
    Entry 1 :
      Vlan id        : 1
      Vlan name      : default

  Protocol ID Entries count : 0
    (None.)

  MAC/PHY Configuration/Status :
    Auto-negotiation support    : supported
    Auto-negotiation status     : enabled
    Auto-negotiation advertised capability : 0005(hex)
    Auto-negotiation operational MAU type : 0010(hex)

  Power Via MDI          :
    Port class           : PSE
    PSE MDI power support : supported
    PSE MDI power state  : enabled
    PSE pairs control ability : uncontrollable
    PSE power pair       : 0
    power class          : 0

  Link Aggregation      :
    Aggregation capability : aggregated

```



```

Aggregation status           : not currently in aggregation
Aggregation port ID         : 0

Maximum Frame Size          : 1536
Unknown TLVs count         : 0
    (None.)

```

```
DES-1228/ME:4#
```

## show lldp statistics

Purpose	Used to display the system LLDP statistics information.
Syntax	<b>show lldp statistics</b>
Description	The global LLDP statistics displays an overview of neighbor detection activity on the switch.
Parameters	None.
Restrictions	None.

### Example usage

To display global statistics information:

```
DES-1228/ME:4# show lldp statistics
```

**Command: show lldp statistics**

```

Last Change Time           : 6094
Number of Table Insert     : 1
Number of Table Delete     : 0
Number of Table Drop       : 0
Number of Table Ageout     : 0

```

```
DES-1228/ME:4#
```

## show lldp statistics ports

Purpose	Used to display the ports LLDP statistics information.
Syntax	<b>show lldp statistics ports{&lt;portlist&gt;}</b>
Description	The per-port LLDP statistics command displays per-port LLDP statistics.
Parameters	<portlist> – Specified a range of ports to be configured. When a port list is not specified, information for all ports will be displayed.
Restrictions	None.

Example usage

To display statistics information of port 1:

```
DES-1228/ME:4# show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID: 1
-----
lldpStatsTxPortFramesTotal      : 27
lldpStatsRxPortFramesDiscardedTotal : 0
lldpStatsRxPortFramesErrors     : 0
lldpStatsRxPortFramesTotal      : 27
lldpStatsRxPortTLVsDiscardedTotal : 0
lldpStatsRxPortTLVsUnrecognizedTotal : 0
lldpStatsRxPortAgeoutsTotal     : 0

DES-1228/ME:4#
```

## PPPoE COMMANDS

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

Command	Parameters
config pppoe circuit_id_insertion state	[enable   disable]
show pppoe circuit_id_insertion	
show pppoe circuit_id_insertion ports	{<portlist>}
config pppoe circuit_id_insertion ports	<portlist> {state [enable   disable]   circuit_id [mac   ip   udf <string 32>]}(1)

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

### config pppoe circuit\_id\_insertion state

Purpose	Used to enable PPPoE circuit ID insertion operations on the switch.
Syntax	<b>config pppoe circuit_id_insertion state [enable   disable]</b>
Description	Used to enable PPPoE circuit ID insertion operations on the switch.
Parameters	<i>state [enable   disable]</i> – The user can enable or disable this option
Restrictions	Only Administrator-level users can issue this command.

#### Example usage

To enable PPPoE circuit ID insertion:

```
DES-1228/ME:4#config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable

Success.

DES-1228/ME:4#
```

### show pppoe circuit\_id\_insertion

Purpose	Used to display PPPoE circuit ID insertion operations on the switch.
Syntax	show pppoe circuit_id_insertion
Description	Used to display PPPoE circuit ID insertion operations on the switch.
Parameters	None
Restrictions	None.

## Example usage

To display PPPoE circuit ID insertion:

```
DES-1228/ME:4#show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Status: Enabled

DES-1228/ME:4#
```

## show pppoe circuit\_id\_insertion ports

Purpose	Used to display PPPoE circuit ID insertion operations on the switch by ports.
Syntax	<b>show pppoe circuit_id_insertion ports {&lt;portlist&gt;}</b>
Description	Used to display PPPoE circuit ID insertion operations on the switch by ports.
Parameters	<portlist> - The user can enter the ports to be used in this field.
Restrictions	None.

## Example usage

To display PPPoE circuit ID insertion by ports:

```
DES-1228/ME:4#show pppoe circuit_id_insertion ports 1-5
Command: show pppoe circuit_id_insertion ports 1-5

Port State      Cirucit ID
-----
1      Enabled  Switch IP
2      Enabled  Switch IP
3      Enabled  Switch IP
4      Enabled  Switch IP
5      Enabled  Switch IP

DES-1228/ME:4#
```

## config pppoe circuit\_id\_insertion ports

Purpose	Used to configure PPPoE circuit ID insertion operations on the switch.
Syntax	<b>config pppoe circuit_id_insertion ports &lt;portlist&gt; {state [enable   disable]   circuit_id [mac   ip   udf &lt;string 32&gt;]}(1)</b>
Description	Used to configure PPPoE circuit ID insertion operations on the switch.
Parameters	<i>ports &lt;portlist&gt;</i> - The user can select a list of ports to include in this configuration. <i>state [enable   disable]</i> – The user can select to enable of disable this feature here. <i>circuit_id [mac ip udf &lt;string 32&gt;]</i> – The user can choose to either use MAC, IP or UDF options and enter an ID for the selected option here.
Restrictions	Only Administrator-level users can issue this command.

Example usage

To configure PPPoE circuit ID insertion:

```
DES-1228/ME:4#config pppoe circuit_id_insertion ports 1-24 state enable circuit_
id ip
Command: config pppoe circuit_id_insertion ports 1-24 state enable circuit_id ip

Success.

DES-1228/ME:4#
```

## 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 binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the DES-1228/ME series, the maximum number of 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	Parameters
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist>   all]}
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist>   all]}
config address_binding ip_mac ports	[<portlist>   all] state [enable   disable] allow_zeroip [enable   disable]
show address_binding	{{ip_mac [all   ipaddress <ipaddr> mac_address <macaddr> ]}blocked [all   vlan_name <vlan_name> mac_address <macaddr>]  ports}}
delete address_binding	[ip_mac [ipaddress <ipaddr> {mac_address <macaddr>}  all]   blocked [all   vlan_name <vlan_name> mac_address <macaddr>]]
enable address_binding trap_log	
disable address_binding trap_log	

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

### create address\_binding ip\_mac ipaddress

Purpose	Used to create an IP-MAC Binding entry.
Syntax	<b>create address_binding ip_mac ipaddress &lt;ipaddr&gt; mac_address &lt;macaddr&gt; {ports [&lt;portlist&gt;   all]}</b>
Description	This command will create an IP-MAC Binding entry.
Parameters	<p>&lt;ipaddr&gt; – The IP address of the device where the IP-MAC binding is made.</p> <p>&lt;macaddr&gt; – The MAC address of the device where the IP-MAC binding is made.</p> <p>&lt;portlist&gt; – Specifies a port or range of ports to be configured for address binding.</p> <p>all – Specifies that all ports on the switch will be configured for address binding.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DES-1228/ME:4#create address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-04
Command: create address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-04

Success.

DES-1228/ME:4#
```

## config address\_binding ip\_mac ipaddress

Purpose	Used to configure an IP-MAC Binding entry.
Syntax	<b>config address_binding ip_mac ipaddress &lt;ipaddr&gt; mac_address &lt;macaddr&gt; {ports [&lt;portlist&gt;   all]}</b>
Description	This command will configure an IP-MAC Binding entry.
Parameters	<p>&lt;ipaddr&gt; – The IP address of the device where the IP-MAC binding is made.</p> <p>&lt;macaddr&gt; – The MAC address of the device where the IP-MAC binding is made.</p> <p>&lt;portlist&gt; – Specifies a port or range of ports to be configured for address binding.</p> <p>all – Specifies that all ports on the switch will be configured for address binding.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-1228/ME:4#config address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-05
Command: config address_binding ip_mac ipaddress 10.1.1.3 mac_address 00-00-00-00-00-05

Success.

DES-1228/ME:4#
```

## config address\_binding ip\_mac ports

Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.
Syntax	<b>config address_binding ip_mac ports [&lt;portlist&gt;   all] state [enable   disable] allow_zeroip [enable   disable]</b>
Description	This command will configure IP-MAC state to enable or disable for specified ports.
Parameters	<p>&lt;portlist&gt; – Specifies a port or range of ports.</p> <p>all – specifies all ports on the switch.</p> <p>state [enable   disable] – Enables or disables the specified range of ports.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DES-1228/ME:4#config address_binding ip_mac ports 2 state enable
```

```
Command: config address_binding ip_mac ports 2 state enable
```

```
Success.
```

```
DES-1228/ME:4#
```

## show address\_binding

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

Example usage:

To show IP-MAC Binding on the switch:



```
DES-1228/ME:4#show address_binding ip_mac all
```

```
Command: show address_binding ip_mac all
```

IP Address	MAC Address	Ports
10.1.1.1	00-00-00-00-00-22	1-28

```
Total Entries: 1
```

```
DES-1228/ME:4#
```

## delete address\_binding

Purpose	Used to delete IP-MAC Binding entries.
Syntax	<b>delete address_binding ip_mac [ipaddress &lt;ipaddr&gt; mac_address &lt;macaddr&gt;   all]   blocked [all   vlan_name &lt;vlan_name&gt; mac_address &lt;macaddr&gt;]]</b>
Description	<p>This command will delete IP-MAC Binding entries. Two different kinds of information can be deleted.</p> <p><i>IP_MAC</i> – Individual Address Binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to <i>all</i> will delete all the Address Binding entries.</p> <p><i>Blocked</i> – 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 <i>all</i>.</p>
Parameters	<p>&lt;ipaddr&gt; – The IP address of the device where the IP-MAC binding is made.</p> <p>&lt;macaddr&gt; – The MAC address of the device where the IP-MAC binding is made.</p> <p>&lt;vlan_name&gt; – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.</p> <p><i>all</i> – For <i>IP_MAC</i> binding <i>all</i> specifies all the IP-MAC binding entries; for Blocked Address Binding entries <i>all</i> specifies all the blocked VLANs and their bound physical addresses.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an IP-MAC Binding on the Switch:

```
DES-1228/ME:4#delete address_binding ip_mac all
```

```
Command: delete address_binding ip_mac all
```

```
Success.
```

```
DES-1228/ME:4#
```

## enable address\_binding trap\_log

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

Example usage:

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

```
DES-1228/ME:4#enable address_binding trap_log
```

```
Command: enable address_binding trap_log
```

```
Success.
```

```
DES-1228/ME:4#
```

## disable address\_binding trap\_log

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

Example usage:

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

```
DES-1228/ME:4#disable address_binding trap_log
```

```
Command: disable address_binding trap_log
```

```
Success.
```

```
DES-1228/ME:4#
```

## LAYER 3 CONTROL PACKET FILTERING

The Layer 3 Control Packet Filtering commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config cpu_filter l3_control_pkt	<portlist> [{dvmrp pim igmp_query ospf rip vrrp}(1)   all] state [enable disable]
show cpu_filter l3_control_pkt	{<portlist>}

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

### config cpu\_filter l3\_control\_pkt

Purpose	This command is used to configure the Layer 3 Control Filter setup of the Switch per port.
Syntax	<b>config cpu_filter l3_control_pkt &lt;portlist&gt; [{dvmrp pim igmp_query ospf rip vrrp}(1)   all] state [enable disable]</b>
Description	This command is used to configure the Layer 3 Control Filter setup of the Switch per port.
Parameters	<p>&lt;portlist&gt; - The user can enter a list of ports to be view here.</p> <p><i>dvmrp   pim   igmp_query   ospf   rip   vrrp</i> – Specify the L3 Control packet to be filtered.</p> <p><i>all</i> – Filter all L3 Control packets. .</p> <p><i>state [enable disable]</i> – The user can set this command’s state to be enabled or disabled.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the Layer 3 Control Filter setup of the Switch per port:

```
DES-1228/ME:4#config cpu_filter l3_control_pkt 1 ospf state enable
Command: config cpu_filter l3_control_pkt 1 ospf state enable

Success.

DES-1228/ME:4#
```

### show cpu\_filter l3\_control\_pkt

Purpose	This command is used to display the Layer 3 Control Filter setup of the Switch per port.
Syntax	<b>show cpu_filter l3_control_pkt {&lt;portlist&gt;}</b>
Description	This command is used to display the Layer 3 Control Filter setup of the Switch per port.
Parameters	<portlist> - The user can enter a list of ports to be view here.
Restrictions	None.

Example usage:

To display the Layer 3 Control Filter setup of the Switch per port:

```
DES-1228/ME:4#show cpu_filter l3_control_pkt 1-5
```

```
Command: show cpu_filter l3_control_pkt 1-5
```

Port	RIP	OSPF	VRRP	PIM	DVMRP	IGMP Query
1	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
2	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled

```
DES-1228/ME:4#
```

## LOOPBACK DETECTION COMMANDS

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

Command	Parameters
config loopdetect	{ recover_timer [0   <value 60-1000000>]   interval <value 1-32767>}(1)
config loopdetect ports	[<portlist>   all] state [enable   disable]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[<portlist>   all]

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

### config loopdetect

Purpose	Used to configure loopback detection on the switch.
Syntax	<b>config loopdetect { recover_timer [0   &lt;value 60-1000000&gt;]   interval &lt;value 1-32767&gt;}(1)</b>
Description	Used to configure loopback detection on the switch.
Parameters	<p><i>recover_timer</i> – The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. The valid range is 60 to 1000000. Zero is a special value which means to disable the auto-recovery mechanism. The default value is 60.</p> <p><i>interval</i> – The time interval (in seconds) at which the remote device transmits all the CTP packets to detect the loopback event. The default value is 10, with a valid range of 1 to 32767.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the recover time to 0, and interval to 20:

```
DES-1228/ME:4#config loopdetect recover_timer 0 interval 20
Command: config loopdetect recover_timer 0 interval 20
```

**Success**

```
DES-1228/ME:4#
```

## config loopdetect ports

Purpose	Used to configure loopback detection on the switch.
Syntax	<b>config loopdetect ports</b> [<portlist>   all]   state [enable   disable]
Description	Used to configure loopback detection on the switch.
Parameters	<portlist> – Specifies a range of ports for the loopback detection state [enable   disable] – Allows the loopback detection to be disabled or enabled.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the loopdetect state to enable:

```
DES-1228/ME:4#config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success

DES-1228/ME:4#
```

## enable loopdetect

Purpose	Used to globally enable loopback detection on the switch.
Syntax	<b>enable loopdetect</b>
Description	Used to globally enable loopback detection on the switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable loop-back detection on the switch:

```
DES-1228/ME:4#enable loopdetect
Command: enable loopdetect

Success

DES-1228/ME:4#
```

## disable loopdetect

Purpose	Used to globally disable loopback detection on the switch.
Syntax	<b>disable loopdetect</b>
Description	Used to globally disable loopback detection on the switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable loop-back detection on the switch:

```
DES-1228/ME:4#disable loopdetect
Command: disable loopdetect

Success

DES-1228/ME:4#
```

## show loopdetect

Purpose	Used to display the current loopback detection settings on the switch.
Syntax	<b>show loopdetect</b>
Description	Used to display the current loopback detection settings on the switch
Parameters	None.
Restrictions	None.

Example usage:

To show loopdetect:

```
DES-1228/ME:4#show loopdetect
Command: show loopdetect

Loopdetect Global Settings
-----
Loopdetect Status      : Enabled
Loopdetect Interval    : 20
Recover Time           : 60

DES-1228/ME:4#
```

## show loopdetect ports

Purpose	Used to display the current per-port loopback detection settings on the switch.
Syntax	<b>show loopdetect ports [&lt;portlist&gt;   all]</b>
Description	Used to display the current per-port loopback detection settings on the switch
Parameters	<portlist> – Specifies a range of ports for the loopback detection all – Specifies all ports for the loopback detection.
Restrictions	None.

Example usage:

To show loopdetect ports:

```
DES-1228/ME:4#show loopdetect ports 1-3
```

```
Command: show loopdetect ports 1-3
```

Port	Loopdetect State	Loop Status
1	Enabled	Normal
2	Enabled	Normal
3	Enabled	Normal

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



## TECHNICAL SUPPORT COMMANDS

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

Command	Parameters
show tech_support	
upload tech_support_to_TFTP	<ipaddr> <path_filename 64>

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

### show tech\_support

Purpose	Used to show the information for technical support.
Syntax	<b>show tech_support</b>
Description	<p>This command is especially used by the technical support personnel to dump the device's overall operation information. The information is project dependent and includes the following information.</p> <ul style="list-style-type: none"> <li>Basic System information</li> <li>system log</li> <li>Running configuration</li> <li>Layer 1 information</li> <li>Layer 2 information</li> <li>Application</li> <li>OS status</li> </ul>
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

## Example usage

To display technical support information on the Switch:

```
DES-1228/ME:4# show tech_support
Command: show tech_support

[Device Information 61450ms]
Device Type       : DES-1228/ME Metro Ethernet Switch
MAC Address       : 00-1B-11-B1-5A-FE
IP Address        : 192.168.69.123 (Manual)
VLAN Name         : default
Subnet Mask       : 255.255.255.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.B01
Firmware Version  : Build 1.00.B04
Hardware Version  : A1
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
802.1x           : Disabled
TELNET            : Enabled(TCP 23)
WEB               : Enabled(TCP 80)
RMON              : Disabled
SSH               : Disabled
Syslog Global State: Disabled
Dual Image        : Supported
Password Encryption Status : Disabled

[CUP Utilization 3049620ms]
CPU Utilization :
-----
Five Seconds -   1 %           One Minute -   1 %           Five Minutes -   2 %

[Connection Session Status 3049620ms]
ID   Login Time           Live Time           From           Level   Name
--   -
8    0/00/00  00:46:34          0:4:14.240     Serial Port     4       Anonymous

Total Entries: 1
[Unicast FDB Table 3049620ms]
VID  MAC Address           Port Type
----  -
1    00-00-00-48-46-29     3    Dynamic
1    00-00-5E-00-01-5F     3    Dynamic
1    00-00-81-00-00-01     3    Dynamic
1    00-00-81-9A-F2-F4     3    Dynamic
1    00-01-01-01-22-22     3    Dynamic
1    00-01-06-30-00-00     3    Dynamic
1    00-01-11-22-33-02     3    Dynamic
1    00-02-A5-FD-66-97     3    Dynamic
1    00-03-09-18-10-01     3    Dynamic
1    00-04-00-00-00-00     3    Dynamic
1    00-05-5D-04-D6-A4     3    Dynamic

Total Entries : 264
```

```
DES-1228/ME:4#
```

## upload tech\_support\_to\_TFTP

Purpose	Used to upload the information of technical support.
Syntax	upload tech_support_to_TFTP <ipaddr> <path_filename>
Description	The upload tech_support_to_TFTP command is used to upload the technical support information.
Parameters	<ipaddr> – Specifies the ipaddress of TFTP server. <path_filename> – Specifies the file path to store the information of technique's support in TFTP server.
Restrictions	Only Administrator-level users can issue this command.

### Example usage

To upload the technical support information:

```
DES-1228/ME:4# upload tech_support_to_tftp 10.55.47.1 tech_report_20080423.txt
Command: upload tech_support_to_tftp 10.55.47.1 tech_report_20080423.txt

Connecting to server..... Done.
Upload technique support information... Done.

Success.
```

## COMMAND HISTORY LIST

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

Command	Parameters
?	
dir	
config command_history	<value 1-40>
show command_history	
enable command logging	
disable command logging	
show command logging	

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

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	? {<command>}
Description	This command will display all of the commands available through the Command Line Interface (CLI).
Parameters	{<command>} – Entering the question mark with an appropriate command will list all the corresponding parameters for the specified command, along with a brief description of the commands function and similar commands having the same words in the command.
Restrictions	None.

## Example usage

To display all of the commands in the CLI:

```
DES-1228/ME:4#?
..
?
cable_diag ports
clear
clear arptable
clear counters
clear fdb
clear flood_fdb
clear igmp_snooping data_driven_group
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display the parameters for a specific command:

```
DES-1228/ME:4#? config stp
Command: ? config stp

Command: config stp
Usage: {maxage <value 6-40>|maxhops <value 6-40> |hellotime <value 1-2>| forwar
ddelay <value 4-30>|txholdcount <value 1-10>|fbpdu [enable|disable]|lbd [enable|
disable] |lbd_recover_timer [<value 0> | <value 60-1000000>]}
Description: Used to setup STP on the switch.
config stp instance_id
config stp mst_config_id
config stp mst_ports
config stp ports
config stp priority
config stp trap
config stp version

DES-1228/ME:4#
```

**dir**

Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	<b>dir</b>
Description	This command will display all of the commands available through the Command Line Interface (CLI).

**dir**

Parameters	None.
Restrictions	None.

Example usage:

To display all commands:

```
DES-1228/ME:4#dir
..
?
clear
clear arptable
clear counters
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config admin local_enable
config arp_aging time
config arpentry
config authen application
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

**config command\_history**

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

Example usage

To configure the command history:

```
DES-1228/ME:4#config command_history 20
Command: config command_history 20

Success.

DES-1228/ME:4#
```

## show command\_history

Purpose	Used to display the command history.
Syntax	<b>show command_history</b>
Description	This command will display the command history.
Parameters	None.
Restrictions	None.

### Example usage

To display the command history:

```
DES-1228/ME:4#show command_history
Command: show command_history

?
? show
show vlan
show command history

DES-1228/ME:4#
```

## enable command logging

Purpose	This command is used to enable command logging.
Syntax	<b>enable command logging</b>
Description	This command is used to enable command logging.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

### Example usage

To enable command logging:

```
DES-1228/ME:4#enable command logging
Command: enable command logging

Success.

DES-1228/ME:4#
```

## show command logging

Purpose	This command is used to display if command logging is enabled or disabled.
Syntax	<b>show command logging</b>
Description	This command is used to display if command logging is enabled or disabled.
Parameters	None.
Restrictions	None.

### Example usage

To display if command logging is enabled or disabled:

```
DES-1228/ME:4#show command logging
Command: show command logging

Command Logging State : Enabled

DES-1228/ME:4#
```

## disable command logging

Purpose	This command is used to disable command logging.
Syntax	<b>disable command logging</b>
Description	This command is used to disable command logging.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

### Example usage

To disable command logging:

```
DES-1228/ME:4#disable command logging
Command: disable command logging

Success.

DES-1228/ME:4#
```



## DHCP SERVER SCREEN LIST

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

Command	Parameters
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> all]   ports [<portlist> all] state [enable   disable]]
config filter dhcp_server trap_log	[enable  disable]
config filter dhcp_server illegal_server_log_suppress_duration	[1min   5min   30min]
show filter dhcp_server	

### config filter dhcp\_server

Purpose	This command is used to configure filtering on the DHCP Server.
Syntax	<b>config filter dhcp_server [add permit server_ip &lt;ipaddr&gt; {client_mac &lt;macaddr&gt;} ports [&lt;portlist&gt; all] delete permit server_ip &lt;ipaddr&gt; {client_mac &lt;macaddr&gt;} ports [&lt;portlist&gt; all]   ports [&lt;portlist&gt; all] state [enable   disable]]</b>
Description	This command is used to configure filtering on the DHCP Server.
Parameters	<i>add permit server_ip &lt;ipaddr&gt;</i> – The user can add a permit server IP address here <i>delete permit server_ip &lt;ipaddr&gt;</i> - The user can delete a permit server IP address here. <i>ports [&lt;portlist&gt; all]</i> – The user can add a defined port list here or select all ports. <i>client_mac &lt;macaddr&gt;</i> - The user can enter the client MAC address in here. <i>state [enable   disable]</i> – The user can enable or disable the state of this command here.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure filtering on the DHCP Server:

```
DES-1228/ME:4#config filter dhcp_server add permit server_ip 10.90.90.10 ports a
ll
Command: config filter dhcp_server add permit server_ip 10.90.90.10 ports all

Success.

DES-1228/ME:4#
```

### config filter dhcp\_server trap\_log

Purpose	This command is used to configure filtering trap logs for the DHCP Server.
Syntax	<b>config filter dhcp_server trap_log [enable  disable]</b>
Description	This command is used to configure filtering trap logs for the DHCP Server.
Parameters	<i>[enable  disable]</i> – The user can enable or disable the trap logs feature in this field.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure filtering trap logs for the DHCP Server:

```
DES-1228/ME:4#config filter dhcp_server trap_log enable
Command: config filter dhcp_server trap_log enable

Success.

DES-1228/ME:4#
```

## config filter dhcp\_server illegal\_server\_log\_suppress\_duration

Purpose	This command is used to configure the filtering illegal server log duration for the DHCP Server.
Syntax	<b>config filter dhcp_server illegal_server_log_suppress_duration [1min   5min   30min]</b>
Description	This command is used to configure the filtering illegal server log duration for the DHCP Server.
Parameters	<i>[1min   5min   30min]</i> – The user can choose from 1, 5 and 30 min for the duration.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the filtering illegal server log duration for the DHCP Server:

```
DES-1228/ME:4#config filter dhcp_server illegal_server_log_suppress_duration 30min
Command: config filter dhcp_server illegal_server_log_suppress_duration 30min

Success.

DES-1228/ME:4#
```

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

## show filter dhcp\_server

Purpose	This command is display the configuration of filtering on the DHCP Server.
Syntax	<b>show filter dhcp_server</b>
Description	This command is display the configuration of filtering on the DHCP Server.
Parameters	None.
Restrictions	None.

Example usage:

To display the configuration of filtering on the DHCP Server:

```
DES-1228/ME:4#show filter dhcp_server
Command: show filter dhcp_server

Enabled ports:
Filter DHCP Server Trap & Log State: Enabled
Illegal_Server_Log_Suppress_Duration : 30 Minutes

Filter DHCP Server/Client Table:
Server IP Address Client MAC address Ports
-----
10.90.90.10                1-28

DES-1228/ME:4#
```

## ARP SPOOFING ATTACK PREVENTION LIST

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

Command	Parameters
config arp_spoofing_prevention	[add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> all]   delete gateway_ip <ipaddr>]
show arp_spoofing_prevention	

### config arp\_spoofing\_prevention

Purpose	This command is used to configure ARP spoofing prevention.
Syntax	<b>config arp_spoofing_prevention [add gateway_ip &lt;ipaddr&gt; gateway_mac &lt;macaddr&gt; ports [&lt;portlist&gt; all]   delete gateway_ip &lt;ipaddr&gt;]</b>
Description	This command is used to configure ARP spoofing prevention.
Parameters	<i>gateway_ip &lt;ipaddr&gt;</i> - The user can enter the Gateway IP address in here. <i>gateway_mac &lt;macaddr&gt;</i> - The user can enter the Gateway MAC address in here. <i>&lt;portlist&gt;</i> - The user can either specify the port(s) or select <i>all</i> ports.
Restrictions	Only Administrator-level users can issue this command.

Example Usage:

To configure ARP spoofing prevention:

```
DES-1228/ME:4#config arp_spoofing_prevention add gateway_ip 10.90.90.1 gateway_mac 00-12-34-56-78-90 ports all
Command: config arp_spoofing_prevention add gateway_ip 10.90.90.1 gateway_mac 00-12-34-56-78-90 ports all
```

Success.

```
DES-1228/ME:4#
```

### show arp\_spoofing\_prevention

Purpose	This command is used to display the ARP spoofing prevention configuration.
Syntax	<b>show arp_spoofing_prevention</b>
Description	This command is used to display the ARP spoofing prevention configuration.
Parameters	None.
Restrictions	None.

Example Usage:

To display ARP spoofing prevention configuration:

```
DES-1228/ME:4#show arp_spoofing_prevention
Command: show arp_spoofing_prevention
```

Gateway IP	Gateway MAC	Ports
-----	-----	-----

10.90.90.1            00-12-34-56-78-90            1-28

Total entries : 1

DES-1228/ME:4#

# Appendix A

## TECHNICAL SPECIFICATIONS

### General

<b>Protocols</b>	<p>IEEE 802.3 10BASE-T Ethernet          IEEE 802.3u 100BASE-TX Fast Ethernet          IEEE 802.3ab 1000BASE-T Gigabit Ethernet          IEEE 802.3z 1000BASE-T (SFP “Mini GBIC”)          IEEE 802.1D/s/w Spanning Tree          IEEE 802.1Q VLAN          IEEE 802.1p Priority Queues          IEEE 802.1X Port Based Network Access Control          IEEE 802.3ad Link Aggregation Control          IEEE 802.3x Full-duplex Flow Control          IEEE 802.3 NWay auto-negotiation</p>												
<b>Fiber-Optic</b>	<p>SFP (Mini GBIC) Support:          DEM-310GT (1000BASE-LX)          DEM-311GT (1000BASE-SX)          DEM-314GT (1000BASE-LH)          DEM-315GT (1000BASE-ZX)          DEM-210 (Single Mode 100BASE-FX)          DEM-211 (Multi Mode 100BASE-FX)</p> <p>WDM Transceivers Supported:          DEM-330T (TX-1550/RX-1310nm), up to 10km, Single-Mode          DEM-330R (TX-1310/RX-1550nm), up to 10km, Single-Mode          DEM-331T (TX-1550/RX-1310nm), up to 40km, Single-Mode          DEM-331R (TX-1310/RX-1550nm), up to 40km, Single-Mode</p>												
<b>Standards</b>	CSMA/CD												
<b>Data Transfer Rates:</b>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"></td> <td style="width: 35%; text-align: center;">Half-duplex</td> <td style="width: 35%; text-align: center;">Full-duplex</td> </tr> <tr> <td><b>Ethernet</b></td> <td style="text-align: center;">10 Mbps</td> <td style="text-align: center;">20Mbps</td> </tr> <tr> <td><b>Fast Ethernet</b></td> <td style="text-align: center;">100Mbps</td> <td style="text-align: center;">200Mbps</td> </tr> <tr> <td><b>Gigabit Ethernet</b></td> <td style="text-align: center;">n/a</td> <td style="text-align: center;">2000Mbps</td> </tr> </table>		Half-duplex	Full-duplex	<b>Ethernet</b>	10 Mbps	20Mbps	<b>Fast Ethernet</b>	100Mbps	200Mbps	<b>Gigabit Ethernet</b>	n/a	2000Mbps
	Half-duplex	Full-duplex											
<b>Ethernet</b>	10 Mbps	20Mbps											
<b>Fast Ethernet</b>	100Mbps	200Mbps											
<b>Gigabit Ethernet</b>	n/a	2000Mbps											
<b>Topology</b>	Star												
<b>Network Cables</b>	<p>Cat.5 Enhanced for 1000BASE-T          UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX          UTP Cat.3, 4, 5 for 10BASE-T          EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)</p>												
<b>Number of Ports</b>	<p>24 x 10/100Base-T Ports          2 x 1000Base-T/SFP Combo Ports          2 x 1000Base-T ports</p>												

### Physical and Environmental

<b>Internal Power Supply</b>	<p>Input: 100~240V, AC/0.5A, 50~60Hz          Output: 12V, 3.3A (Max)</p>
------------------------------	---

<b>Power Consumption</b>	18.8W
<b>DC Fans</b>	None
<b>Operating Temperature</b>	0 - 40°C
<b>Storage Temperature</b>	-40 - 70°C
<b>Humidity</b>	5 - 95% non-condensing
<b>Dimensions</b>	441(W) x 207(D) x 44(H) mm
<b>Weight</b>	2.36kg (5.20lbs)

### Performance

<b>Transmission Method</b>	Store-and-forward
<b>Packet Buffer</b>	512 KB per device
<b>Packet Filtering/ Forwarding Rate</b>	14,881 pps (10M port) 148.810 pps (100M port) 1,488,100 pps (1Gbps port)
<b>MAC Address Learning</b>	Automatic update. Supports 8K MAC address
<b>Priority Queues</b>	4 Priority Queues per port.
<b>Forwarding Table Age Time</b>	Max age: 10-1000000 seconds. Default = 300.

### LED Indicators

Location	LED Indicative	Color	Status	Description
Per Device	Power	Green	Solid Light	Power On
			Light off	Power Off
	Console	Green	Solid Light	Console on
			Blinking	POST is in progress/ POST is failure.
			Light off	Console off
LED Per 10/100 Mbps Port	Link/Act/Speed	Green/Amber	Solid Green	When there is a secure 100Mbps Fast Ethernet connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a Fast Ethernet connected port.
			Solid Amber	When there is a secure 10Mbps Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at an Ethernet connected port.
			Light off	No link
LED Per GE Port	Link/Act/Speed mode for 1000BASE-T	Green/Amber	Solid Green	When there is a secure 1000Mbps connection (or link) at any of the ports.

	<b>ports</b>		Blinking Green	When there is reception or transmission (i.e. Activity--Act) of data occurring at a 1000Mbps connected port.
			Solid Amber	When there is a secure 10/100Mbps Fast Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at a Fast Ethernet connected port.
			Light off	No link
	<b>Link/Act/Speed mode for SFP ports</b>	Green/Amber	Solid Green	When there is a secure 1000Mbps connection (or link) at the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity--Act) of data occurring at a 1000Mbps connected port.
			Solid Amber	When there is a secure 100Mbps connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at the ports.
			Light off	No link

### Power

Feature	Detailed Description
Internal Power Supply	AC Input: 100 - 240 VAC, 50-60 Hz

### Performance

Feature	Detailed Description
Wire speed on all FE/GE ports	Full-wire speed (full-duplex) operation on all FE/GE ports
Forwarding Mode	Store and Forward
Switching Capacity	12.8Gbps
64 Byte system packet forwarding rate	9.5 million packets per second
Priority Queues	4 Priority Queues per port
MAC Address Table	Supports 8K MAC address
Packet Buffer Memory	512K Bytes

### Port Functions

Feature	Detailed Description
Console Port	DCE RS-232 DB-9 for out-of-band configuration of the software features



24 x 10/100BaseT ports	<p>Compliant to following standards,  IEEE 802.3 compliance  IEEE 802.3u compliance  Support Half/Full-Duplex operations  All ports support Auto MDI-X/MDI-II cross over  IEEE 802.3x Flow Control support for Full-Duplex mode, Back Pressure when Half-Duplex mode, and Head-of-line blocking prevention.</p>
Combo ports in the front panel	<p>combo 1000BASE-T/SFP ports</p> <p>1000BASE-T ports compliant to following standards:  IEEE 802.3 compliance  IEEE 802.3u compliance  IEEE 802.3ab compliance  Support Full-Duplex operations  IEEE 802.3x Flow Control support for Full-Duplex mode, back pressure when Half-Duplex mode, and Head-of-line blocking prevention</p> <p>SFP Transceivers Supported:  DEM-310GT (1000BASE-LX)  DEM-311GT (1000BASE-SX)  DEM-314GT (1000BASE-LH)  DEM-315GT (1000BASE-ZX)  DEM-210 (Single Mode 100BASE-FX)  DEM-211 (Multi Mode 100BASE-FX)</p> <p>-WDM Transceiver Supported:  1.DEM-330T (TX-1550/RX-1310nm), up to 10km, Single-Mode  2.DEM-330R (TX-1310/RX-1550nm), up to 10km, Single-Mode  3.DEM-331T (TX-1550/RX-1310nm), up to 40km, Single-Mode  4.DEM-331R (TX-1310/RX-1550nm), up to 40km, Single-Mode</p> <p>Compliant to following standards:  IEEE 802.3z compliance  IEEE 802.3u compliance</p>
1000BASE-T ports in the front panel	<p>1000BASE-T ports compliant to following standards:</p> <ol style="list-style-type: none"> <li>1. IEEE 802.3 compliance</li> <li>2. IEEE 802.3u compliance</li> <li>3. IEEE 802.3ab compliance</li> <li>4. Support Full-Duplex operations</li> <li>5. IEEE 802.3x Flow Control support for Full-Duplex mode, back pressure when Half-Duplex mode, and Head-of-line blocking prevention</li> </ol>

**Pin Assignment for Data: (alternative A MDI-X)**

PIN#	Signal
1	Receive+
2	Receive-
3	Transmit+
4	
5	
6	Transmit-
7	
8	