D-Link®

DES-3250TG

Layer 2 Switch

Command Line Interface
Reference Manual

Second Edition (October 2003)

6ES3250TGC03

Printed In Taiwan

RECYCLABLE

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.

2. Heben Sie diese Anleitung für den spätern Gebrauch auf.

3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.

4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.

5. Das Gerät is vor Feuchtigkeit zu schützen.

6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.

7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.

8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.

9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.

10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.

11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.

12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.

13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.

14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.

15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:

    a – Netzkabel oder Netzstecker sint beschädigt.

    b – Flüssigkeit ist in das Gerät eingedrungen.

c – Das Gerät war Feuchtigkeit ausgesetzt.

d – Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.

e – Das Gerät ist gefallen und|oder das Gehäuse ist beschädigt.

f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.

16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.

17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.

18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing|shipping|insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this

warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system|platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system|platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address|telephone|fax|e-mail|Web site list of D-Link offices is provided in the back of this manual.

Trademarks

Copyright Statement

FCC Warning

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

CE Mark Warning

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

VCCI Warning

注意
この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI Warning

警告使用者
這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,在這種情況下使用者會被要求採取某些適當的對策.

Table of Contents

1

INTRODUCTION

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

This manual provides a reference for all of the commands contained in the CLI. Configuration and management of the switch via the Web-based management agent is discussed in the 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 is then connected to the switch's serial port via an RS-232 DB-9 cable.

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

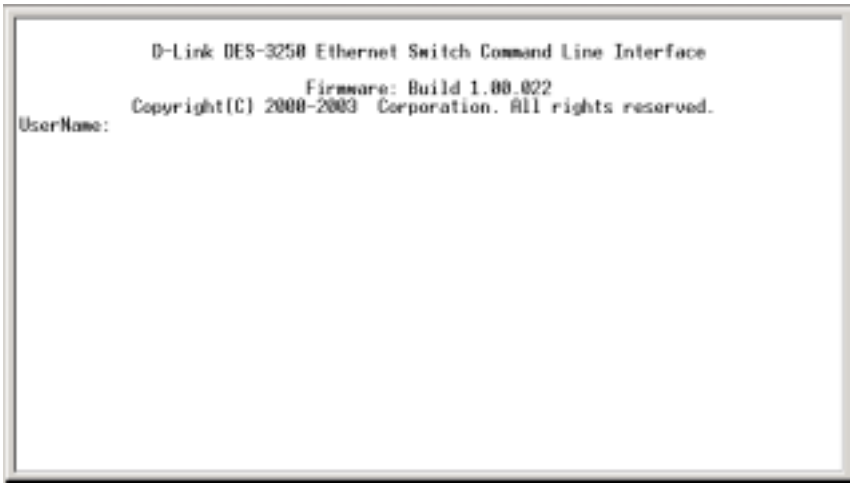


Figure 1-1. Initial Console screen.

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **local>**. This is the command line where all commands are input.

Setting the Switch's IP Address

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

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

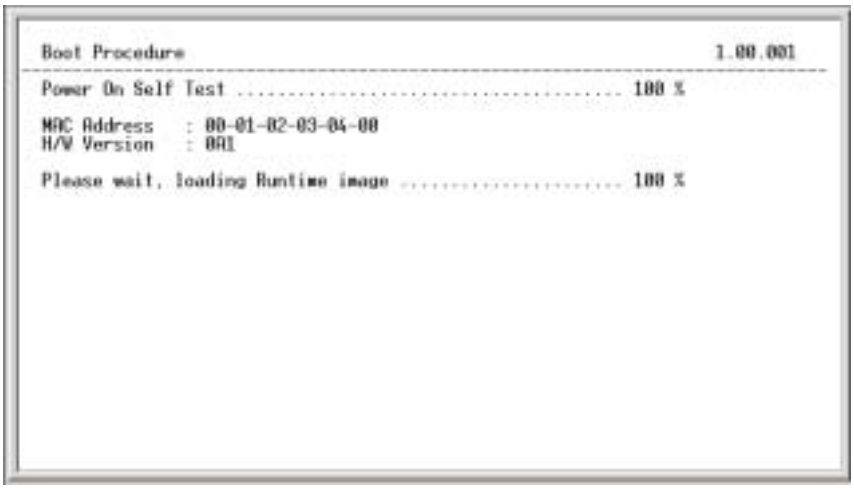


Figure 1-2. Boot Screen

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

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

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

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

2. Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx|z**. Where the **x**'s represent the IP

address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

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

Figure 1-3. Assigning the Switch an IP Address

In the above example, the switch was assigned an IP address of 10.24.22.5 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 and the CLI or via the Web-based management agent using the above IP address to connect to the switch.

2

USING THE CONSOLE CLI

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

Switch configuration settings are saved to non-volatile RAM using *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
- 9,600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

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

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

Figure 2-1. Initial Console Screen

Commands are entered at the command prompt, **local>**.

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

Figure 2-2. The ? Command

The **dir** command has the same function as the **?** command.

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

Alternatively, if you hit the **Tab** key immediately after you have entered a command, the CLI will display all the next available parameters sequentially.

Figure 2-3. Example Command Parameter Help

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

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

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

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

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

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

Figure 2-5. The Available Commands Prompt

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

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

Figure 2-6. Next possible completions: Show Command

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

3

COMMAND SYNTAX

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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**configure ipif System ipaddress <network_address>**
Description	In the above syntax example, you must supply the network address in the <network_address> space. Do not type the angle brackets.
Example Command	**configure ipif System ipaddress 10.24.22.5/255.0.0.0**

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One or more values or arguments can be specified.

[square brackets]	
Syntax	**create account [admin|user]**
Description	In the above syntax example, you must specify either an admin or a user level account to be created. Do not type the square brackets.
Example Command	**create account admin**

|vertical bar	
Purpose	Separates two or more mutually exclusive items in a list – one of which must be entered.
Syntax	**show snmp [community|trap receiver]**
Description	In the above syntax example, you must specify either community, trap receiver, or detail. Do not type the vertical bar.
Example Command	**show snmp community**

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	**config serial_port** **{baud_rate[9600|19200|38400|115200]|** **auto_logout** **[never|2_minutes|5_minutes|** **10_minutes|15_minutes]}**

{braces}	
Description	In the above syntax example, baud_rate, auto_logout, never, 2_minutes, 5_minutes, 10_minutes, and 15_minutes are all optional arguments. You can specify any or all of the arguments contained by braces. Do not type the braces.
Example command	**config serial_port baud_rate 9600**

Line Editing Key Usage	
Delete	Deletes character under the cursor.
Backspace	Deletes the character to the left of the cursor and shifts the remaining characters in the line to the left.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Tab	Displays all the next parameters sequentially.

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 displaying.
a	Displays the remaining pages without pausing between pages.
Enter	Displays the next line or table entry.

4

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin|user] <username>
config account	<username>
show account	
delete account	
show session	
show switch	
show serial_port	
config serial_port	baud_rate [9600|19200|38400|115200] auto_logout [never|2_minutes|5_minutes |10_minutes|15_minutes]
enable clipaging	
disable clipaging	

Command	Parameters
enable telnet	<tcp_port_number>
disable telnet	
enable web	<tcp_port_number>
disable web	
save	
reboot	
reset	{[config|system]}
login	
logout	

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

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

Example Usage:

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

```
local>create account admin dlink
Command: create account admin dlink

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

```
local>
```

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

Example Usage:

To configure the user password of "dlink" account:

```
local>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.

local>
```

show account	
Purpose	Used to display user accounts
Syntax	**show account**
Description	Displays all user accounts created on the switch. Up to eight user accounts can exist on the switch at one time.
Parameters	none.
Restrictions	none.

Example Usage:

To display the accounts which have been created:

```
local>show account
Command: show account

 Current Accounts:
   Username         Access Level
 ---------------    ------------
  dlink               Admin
local>
```

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

Example Usage:

To delete the user account "System":

```
local>delete account System
Command: delete account System

 Success.

local>
```

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

Example Usage:

To display the way that the users logged in:

```
local>show session

ID   Live Time     From          Level   Name
---  ------------  ------------  -------  ----------------
8    0:17:16.2     Serial Port   4        Anonymous
local>
```

show switch	
Purpose	Used to display information about the switch.
Syntax	**show switch**
Description	This command displays information about the switch.
Parameters	none.
Restrictions	none.

Example Usage:

To display the switch information:

```
local>show switch
Command: show switch

Device Type          : DES-3250 Fast-Ethernet Switch
Ext. Ports           : 1000TX + 1000TX
MAC Address          : 00-01-02-03-04-00
IP Address           : 10.90.90.90 (Manual)
VLAN Name            : default
Subnet Mask          : 255.0.0.0
Default Gateway      : 0.0.0.0
Boot PROM Version    : Build 1.00.002
Firmware Version     : Build 2.00.017
Hardware Version     : 0A1
System Up  Time      : 0 days 00:47:09
Time                 : Unknown
```

```
Time Source          : System Clock
System Name          :
System Location      :
System Contact       :
Spanning Tree        : Disabled
GVRP                 : Disabled
IGMP Snooping        : Disabled
TELNET               : Enabled  (TCP 23)
SNTP                 : Disabled
WEB                  : Enabled  (TCP 80)
RMON                 : Disabled
local>
```

show serial_port	
Purpose	Used to display the current serial port settings.
Syntax	**show serial_port**
Description	This command displays the current serial port settings.
Parameters	none.
Restrictions	none

Example Usage:

To display the serial port setting:

```
local>show serial_port
Command: show serial_port

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

local>
```

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

Example Usage:

To configure baud rate:

```
local>config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600
 Success.
local>
```

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

```
local>enable clipaging
Command: enable clipaging
 Success.

local>
```

disable clipaging	
Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when the show command would display more than one screen of information.
Syntax	**disable clipaging**
Description	This command is used to disable the pausing of the console screen at the end of each page when the show 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:

```
local>disable clipaging
Command: disable clipaging
 Success.
local>
```

enable telnet	
Purpose	Used to enable communication with and management of the switch using the Telnet protocol.
Syntax	**enable telnet <tcp_port_number>**
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> – 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:

```
local>enable telnet 23
Command: enable telnet 23
 Success.
local>
```

disable telnet	
Purpose	Used to disable the Telnet protocol on the switch.
Syntax	**disable telnet**
Description	This command is used to disable the Telnet protocol on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable the Telnet protocol on the switch:

```
local>disable telnet
Command: disable telnet
 Success.

local>
```

enable web	
Purpose	Used to enable the HTTP-based management software on the switch.
Syntax	**enable web <tcp_port_number>**
Description	This command is used to enable the Web-based management software on the switch. The user can specify the TCP port number the switch will use to listen for Telnet requests.
Parameters	<tcp_port_number> – 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:

```
local>enable web 80
Command: enable web 80
 Success.

local>
```

disable web	
Purpose	Used to disable the HTTP-based management software on the switch.
Syntax	**disable web**
Description	This command disables the Web-based management software on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable HTTP:

```
local>disable web
Command: disable web
 Success.

local>
```

save	
Purpose	Used to save changes in the switch's configuration to non-volatile RAM.
Syntax	**save**
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the switch's memory each time the switch is restarted.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
local>save
Command: save

Saving all settings to NV-RAM...   100%
done.
local>
```

reboot	
Purpose	Used to restart the switch.
Syntax	**reboot**
Description	This command is used to restart the switch.
Parameters	none.
Restrictions	none.

Example Usage:

To restart the switch:

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

reset	
Purpose	Used to reset the switch to the factory default settings.
Syntax	**reset {[config|system]}**
Description	This command is used to restore the switch's configuration to the default settings assigned from the factory.
Parameters	config – If config is specified, all of the factory default settings are restored on the switch except for the IP address, user accounts, and the switch history log. system – If system is specified all of the factory default settings are restored on the switch. If no parameter specified, the switch's current IP address, user accounts, and switch history log are retained. All other parameters are restored to their factory default settings.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
local>reset config
Command: reset config
 Success.

local>
```

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

Example Usage:

To initiate the login procedure:

```
local>login
Command: login

UserName:
```

logout	
Purpose	Used to log out a user from the switch's console.
Syntax	**logout**
Description	This command terminates the current user's session on the switch's console.
Parameters	none.
Restrictions	none.

Example Usage:

To terminate the current user's console session:

```
local>logout
```

5

SWITCH PORT COMMANDS

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

Command	Parameters
config ports	<portlist|all> speed [auto|10_half|10_full|100_half|100_full| 1000_half|1000_full] learning [enabled|disabled] state [enabled|disabled]
show ports	<portlist|all>

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

config ports	
Purpose	Used to configure the switch's Ethernet port settings.
Syntax	**config ports [<portlist|all>] {speed** **[auto|10_half|10_full|100_half|100_full|** **1000_half|1000_full]** **learning [enabled|disabled]** **state [enabled|disabled]}**
Description	This command allows for the configuration of the switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.
Parameters	all – Displays all ports on the switch to be configured. portlist – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. auto – Enables auto-negotiation for the specified range of ports. [10|100|1000] – Configures the speed in Mbps for the specified range of ports. [half|full] – Configures the specified range of ports as either full- or half-duplex. learning [enabled|disabled] – Enables or disables the MAC address learning on the specified range of ports. state [enabled|disabled] – Enables or disables the specified range of ports.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
local>config ports 1-3 speed 10_full learning enabled state enabled

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

Success.
```

show ports	
Purpose	Used to display the current configuration of a range of ports.
Syntax	**show ports {<portlist|all>}**
Description	This command is used to display the current configuration of a range of ports.
Parameters	all – Displays all ports on the switch. <portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	none.

Example Usage:

To display the configuration of the ports 1-7:

```
local>show ports 1-7
Command: show ports 1-7

Port  Port        Settings              Connection            Address
      State       Speed|Duplex          Speed|Duplex          Learning
----  --------    --------------------  --------------------  -----------
1     Enabled     Auto                  Link Down             Enabled
2     Enabled     Auto                  Link Down             Enabled
```

3	Enabled	Auto	Link Down	Enabled
4	Enabled	Auto	Link Down	Enabled
5	Enabled	Auto	Link Down	Enabled
6	Enabled	Auto	Link Down	Enabled
7	Enabled	Auto	Link Down	Enabled

6

PORT SECURITY COMMANDS

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

Command	Parameters
config port_security ports	[<portlist>|all] {admin_state [enable | disable] |max_learning_addr <max_lock_no 0-10>|lock_address_mode [DeleteOnTimeout|DeleteOnReset]}
show port_security	{ports <portlist>}

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

config port_security ports	
Purpose	Used to configure port security settings.
Syntax	**config port_security ports [<portlist>| all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-10> | lock_address_mode [DeleteOnTimeout|DeleteOnReset]}**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <portlist> are effected.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – configure port security for all ports on the switch. admin_state [enabled|disaled] – enable or disable port security for the listed ports. max_learning_addr <1-10> - use this to limit the number of MAC addresses dynamically listed in the FDB for the ports. lock_address_mode[DeleteOnTimout|DeleteOnReset] – delete FDB dynamic entries for the ports on timeout of the FDB (see Forwarding Database Commands). Specify DeleteOnReset to delete all FDB entries, including static entries upon system reset or rebooting.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the port security:

```
local>config port_security ports 5-6 admin_state enable max_learning_addr
5 lock_address_mode DeleteOnTimeout

Command: config port_security ports 5-6 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnTimeout


Success


local>
```

show port_security	
Purpose	Used to display the current port security configuration.
Syntax	**show port_security {ports <portlist>}**
Description	This command is used to display port security information of the switch ports. The information displayed includes port security admin state, maximum number of learning address and lock mode.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	none.

Example usage:

To display the port security configuration:

```
local>show port_security
Command: show port_security

 Port#  Admin State  Max. Learning Addr.  Lock Address Mode
 ----   -----------  -------------------  -----------------
 1      Disabled     1                    DeleteOnReset
 2      Disabled     1                    DeleteOnReset
 3      Disabled     1                    DeleteOnReset
```

4	Disabled	1	DeleteOnReset
5	Disabled	1	DeleteOnReset
6	Disabled	1	DeleteOnReset
7	Enabled	10	DeleteOnReset
8	Disabled	1	DeleteOnReset
9	Disabled	1	DeleteOnReset
10	Disabled	1	DeleteOnReset
11	Disabled	1	DeleteOnReset
12	Disabled	1	DeleteOnReset
13	Disabled	1	DeleteOnReset
14	Disabled	1	DeleteOnReset
15	Disabled	1	DeleteOnReset
16	Disabled	1	DeleteOnReset
17	Disabled	1	DeleteOnReset
18	Disabled	1	DeleteOnReset
19	Disabled	1	DeleteOnReset
20	Disabled	1	DeleteOnReset

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

7

NETWORK MANAGEMENT COMMANDS

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

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

SNMP Version	Authentication Method	Description
v1	Community String	Community String is used for authentication – NoAuthNoPriv
v2c	Community String	Community String is used for authentication – NoAuthNoPriv
v3	Username	Username is used for authentication – NoAuthNoPriv
v3	MD5 or SHA	Authentication is based on the HMAC-MD5 or HMAC-SHA algorithms – AuthNoPriv

v3	MD5 DES or SHA DES	Authentication is based on the HMAC-MD5 or HMAC-SHA algorithms – AuthPriv. DES 56-bit encryption is added based on the CBC-DES (DES-56) standard

Command	Parameters
enable rmon	
disable rmon	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable snmp traps	
disable snmp traps	
enable snmp authenticate traps	
disable snmp authenticate traps	
create trusted_host	<ipaddr>
show trusted_host	<ipaddr>

Command	Parameters
delete trusted_host	<ipaddr>
ping	<ipaddr> times <value> timeout <sec>
create snmp user	<username 32> <groupname 32> {encrypted (1) [by_password(1) auth[md5(2) <auth_password 8-16 > | sha(3) <auth_password 8-20 >] priv [none(1) | des(2) <priv_password 8-16>]| by_key(2) auth [md5(2) <auth_key 32-32>| sha(3) <auth_key 40-40>] priv [none(1) |des(2) <priv_key 32-32>]]}
delete snmp user	<username 32>
show snmp user	
show snmp groups	
create snmp view	<view_name 32> <oid> view_type [included|excluded]
delete snmp view	<view_name 32> [all | <oid>]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only|read_write]
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID>
show snmp	

Command	Parameters
engineID	
create snmp group	<groupname 32> [v1|v2c|v3 [noauth_nopriv|auth_nopriv|auth_priv]]{read_view <view_name 32> | write_view <view_name 32> |notify_view <view_name 32>}
delete snmp group	<groupname 32>
create snmp host	<ipaddr> [v1|v2c|v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	{<ipaddr>}

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

config snmp system_name	
Purpose	Used to configure a name for the switch.
Syntax	**config snmp system_name <sw_name>**
Description	This command is used to give the switch an alpha-numeric name of up to 255 characters.
Parameters	<sw_name> – An alpha-numeric name for the switch of up to 255 characters.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the switch name for "DES-3250":

```
local>config snmp system_name DES3250
Command: config snmp system_name DES3250
Success.
local>
```

config snmp system_location	
Purpose	Used to enter a description of the location of the switch.
Syntax	**config snmp system_location <sw_location>**
Description	This command is used to enter a description of the location of the switch. A maximum of 255 characters can be used.
Parameters	<sw_location> – A description of the location of the switch. A maximum of 255 characters can be used.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the switch location for "Taiwan":

.

```
local>config snmp system_location Taiwan
Command: config snmp system_location Taiwan
Success.
local>
```

config snmp system_contact	
Purpose	Used to enter the name of a contact person who is responsible for the switch.
Syntax	**config snmp system_contact <sw_contact>**
Description	This command is used to enter the name and|or other information to identify a contact person who is responsible for the switch. A maximum of 255 characters can be used.
Parameters	<sw_contact> – A maximum of 255 characters used to identify a contact person who is responsible for the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the switch contact to "ctsnow":

.

```
local>config snmp system_contact ctsnow
Command: config snmp system_contact ctsnow
Success.
local>
```

enable rmon	
Purpose	Used to enable RMON on the switch.
Syntax	**enable rmon**
Description	This command is used, in conjunction with the disable RMON command below, to enable and disable remote monitoring (RMON) on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable RMON:

```
local>enable rmon
Command: enable rmon
Success.

local>
```

disable rmon	
Purpose	Used to disable RMON on the switch.
Syntax	**disable rmon**
Description	This command is used, in conjunction with the enable rmon command above, to enable and disable remote monitoring (RMON) on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable RMON:

```
local>disable rmon
Command: disable rmon
 Success.

local>
```

create trusted_host	
Purpose	Used to create trusted hosts.
Syntax	**create trusted_host <ipaddr>**
Description	This command is used to create trusted hosts. A trusted host is a recipient of SNMP, Web, and Telnet messages generated by the switch's SNMP agent.
Parameters	<ipaddr> – The IP address of the trusted host.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create a trusted host:

```
local>create trusted_host
Command: create trusted_host 10.1.1.1
 Success.

local>
```

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

Example Usage:

To display the list of trusted hosts:

```
local>show trusted_host
Command: show trusted_host

 Management Stations
 IP Address:
-------------------------
10.1.1.1
Total Entries:  1

local>
```

delete trusted_host	
Purpose	Used to delete a trusted host entry made using the create trusted_host command above.
Syntax	**delete trusted _host <ipaddr>**
Description	This command is used to delete a trusted host entry made using the create trusted_host command above.
Parameters	<ipaddr> – The IP address of the trusted host.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

```
local>delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

local>
```

enable snmp traps	
Purpose	Used to enable SNMP trap support.
Syntax	**enable snmp traps**
Description	This 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 turn on SNMP trap support:

```
local>enable snmp traps
Command: enable snmp traps
Success.

local>
```

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

Example Usage:

To prevent SNMP traps from being sent from the switch:

```
local>disable snmp traps
Command: disable snmp traps
Success.
local>
```

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

Example Usage:

To turn on SNMP authentication trap support:

```
local>enable snmp authenticate traps
Command: enable snmp authenticate traps

 Success.

local>
```

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

Example Usage:

To turn off SNMP authentication trap support:

```
local>disable snmp authenticate traps
Command: disable snmp authenticate traps
 Success.

local>
```

ping	
Purpose	Used to test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value>} {timeout <sec>}**
Description	This command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then "echo" or return the message. This is used to confirm connectivity between the switch and the remote device.
Parameters	<ipaddr> – The IP address of the remote device. times <value> – The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0. timeout <sec> – Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To send ICMP echo message to "10.48.74.121" for four times:

```
local>#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

local>
```

create snmp user	
Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	**create snmp user <username 32> <groupname 32> {encrypted (1) [by_password(1) auth[md5(2) <auth_password 8-16 > | sha(3) <auth_password 8-20 >]priv [none(1) | des(2) <priv_password 8-16>]| by_key(2) auth [md5(2) <auth_key 32-32>| sha(3) <auth_key 40-40>]priv [none(1) |des(2) <priv_key 32-32>]]}**
Description	The create snmp user command creates a new SNMP user and adds the user to an SNMP group that is also created by this command.
Parameters	<username 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP user. <groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. encrypted – Specifies that the password will be in an encrypted format. by_password – Indicate input password for authentication and privacy. by_key – Indicate input key for authentication and privacy. auth – Initiates an authentication level setting session. The options are MD5 and SHA. md5 – The HMAC-MD5-96 authentication level.

create snmp user	
	sha – The HMAC-SHA-96 authentication level. <auth_password 8-16> – An alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host. <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. <auth_key> – An authentication key used by MD5 or SHA1, it is hex string type. <priv_key> – A privacy key used by DES, it is hex string type.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP user on the switch:

```
local>create snmp user dlink default encrypted by_password
auth md5 auth_password none

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

Success.


local>
```

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

Example Usage:

To delete a previously entered SNMP user on the switch:

```
local>delete snmp user dlink
Command: delete snmp user dlink
 Success.
local>
```

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

Example Usage:

To display the SNMP users currently configured on the switch:

```
local>show snmp user
Command: show snmp user

Username                        Group Name       Ver   Auth    Priv
------------------------------  ---------------  ----- ------- ------------
initial                         initial          V3    None    None

Total Entries: 1

local>
```

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

Example Usage:

To display the currently configured SNMP groups on the switch:

```
local>show snmp groups
Command: show snmp groups
Vacm Access Table Settings

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

Group    Name      : ReadGroup
```

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

Total Entries: 2

local>
```

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

Example Usage:

To create an SNMP view:

```
local>create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included
 Success.
local>
```

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

Example Usage:

To delete a previously configured SNMP view from the switch:

```
local>delete snmp view dlinkview
Command: delete snmp view dlinkview

 Success.

local>
```

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

Example Usage:

To show SNMP view:

```
local>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       .3.6.1.6.3.1            Included

Total Entries: 11

local>
```

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

create snmp community	
	group of MIB objects that a remote SNMP manager is allowed to access on the switch. read_only – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the switch. read_write – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create the SNMP community string "dlink:"

```
local>create snmp community dlink view ReadView read_write

Command: create snmp community dlink view ReadView
read_write


 Success.

local>
```

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

Example Usage:

To delete the SNMP community string "dlink:"

```
local>delete snmp community dlink
Command: delete snmp community dlink
 Success.
local>
```

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

Example Usage:

To display the currently entered SNMP community strings:

```
local>show snmp community

Command: show snmp community

 SNMP Community Table

 Community Name      View Name              Access Right

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

 dlink               ReadView               read_write

 private             CommunityView          read_write

 public              CommunityView          read_only

Total Entries: 3

local>
```

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

Example Usage:

To give the SNMP agent on the switch the name "0035636666:"

```
local>config snmp 0035636666
Command: config snmp engineID 0035636666
 Success.
local>
```

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

Example Usage:

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

```
local>show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

local>
```

create snmp group	
Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	**create snmp group <groupname 32> [v1|v2c|v3 [noauth_nopriv|auth_nopriv|auth_priv]] {read_view <view_name 32>|write_view <view_name 32>|notify_view <view_name 32>}**
Description	The create snmp group command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	<groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: Message integrity – ensures that packets have

create snmp group	
	not been tampered with in transit. Authentication – determines that an SNMP message is from a valid source. Encryption – scrambles the contents of messages to prevent it being seen by an unauthorized source. noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager. auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager. auth_priv – Specifies that authorization will be required, and that packets sent between the swtich and a remote SNMP manger will be encrypted. read_view – Specifies that the SNMP group being created can request SNMP messages. <view_name 32> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch. notify_view – Specifies that the SNMP group being created can recieve SNMP trap messages generated by the switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP group named "sg1:"

```
local>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.


local>
```

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

Example Usage:

To delete the SNMP group named "sg1".

```
local>delete snmp group sg1
Command: delete snmp group sg1
 Success.
local>
```

create snmp host	
Purpose	Used to create a recipient of SNMP traps generated by the switch's SNMP agent.
Syntax	**create snmp host <ipaddr> [v1|v2c|v3 [noauth_nopriv|auth_nopriv|auth_priv]] <auth_string 32>**
Description	The create snmp host command creates a recipient of SNMP traps generated by the switch's SNMP agent.
Parameters	<ipaddr> – The IP address of the remote management station that will serve as the SNMP host for the switch. v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: Message integrity – ensures that packets have not been tampered with in transit. Authentication – determines that an SNMP message is from a valid source.

create snmp host	
	Encryption – scrambles the contents of messages to prevent it being seen by an unauthorized source. noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager. auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager. auth_priv – Specifies that authorization will be required, and that packets sent between the swtich and a remote SNMP manger will be encrypted. <auth_sting 32> – An alphanumeric string used to authorize a remote SNMP manager to access the switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP host to receive SNMP messages:

```
local>create snmp host 10.48.74.100 v3 auth_priv public
Command: create snmp host 10.48.74.100 v3 auth_priv public
 Success.

local>
```

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

Example Usage:

To delete an SNMP host entry:

```
local>delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100
 Success.

local>
```

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

Example Usage:

To display the currently configured SNMP hosts on the switch:

```
local>show snmp host
Command: show snmp host

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

Total Entries: 2
```

9

DOWNLOAD/UPLOAD COMMANDS

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

Command	Parameters
download	firmware <ipaddr> <path_filename 64> configuration <ipaddr> <path_filename 64> {increment}
upload	configuration log <ipaddr> <path_filename 64>

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

download	
Purpose	Used to download and install new firmware or a switch configuration file from a TFTP server.
Syntax	**download [firmware <ipaddr> <path_filename 64> |configuration <ipaddr> <path_filename 64> {increment}]**
Description	This command is used to download a new firmware or a switch configuration file from a TFTP server.
Parameters	firmware – Download and install new firmware on the switch from a TFTP server. configuration – Download a switch configuration file from a TFTP server. <ipaddr> – The IP address of the TFTP server. <path_filename 64> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3250.had. increment – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
Restrictions	The TFTP server must be on the same IP subnet as the switch. Only administrator-level users can issue this command.

Example Usage:

```
local>download configuration 10.48.74.121 c:\cfg\setting.txt
Command: download configuration 10.48.74.121 c:\cfg\setting.txt

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

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

Example Usage:

```
local>upload configuration 10.48.74.121 c:\cfg\log.txt
Command: upload configuration 10.48.74.121 c:\cfg\log.txt

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

local>
```

10

NETWORK MONITORING COMMANDS

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

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilitzation	
clear counters	ports <portlist>
clear log	
show log	index <value>
enable syslog	
disable syslog	
show syslog	
create syslog host	all <index 1-4> severity informational warning

Command	Parameters
	all facility local0 local1 local2 local3 local4 local5 local6 local7 udp_port <udp_port_number> ipaddress <ipaddr> state [enabled|disabled]
config syslog host	all <index 1-4> severity informational warning all facility local0 local1 local2 local3 local4 local5 local6

Command	Parameters
	local7 udp_port <udp_port_number> ipaddress <ipaddr> state [enabled|disabled]
delete syslog host	<index 1-4> all
show syslog host	<index 1-4>

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

show packet ports	
Purpose	Used to display statistics about the packets sent and received by the switch.
Syntax	**show packet ports <portlist>**
Description	This command is used to display statistics about packets sent and received by ports specified in the port list.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example usage:

To display the packets analysis for ports 1 through 7:

```
local>show packet ports 1-7
Port number : 1-7
Frame Size    Frame Counts  Frames|sec    Frame Type    Total
Total|sec
------------  ------------  ----------    ----------    -------  ---------
64              3275          10          RX Bytes      408973   1657
65-127           755          10          RX Frames       4395     19
128-255          316           1
256-511          145           0          TX Bytes        7918    178
512-1023          15           0          TX Frames        111      2
1024-1518          0           0
Unicast RX       152           1
Multicast RX     557           2
Broadcast RX    3686          16

Broadcast RX    4495          42

local>
```

show error ports	
Purpose	Used to display the error statistics for a range of ports.
Syntax	**show error ports <portlist>**
Description	This command will display all of the packet error statistics collected and logged by the swtich for a given port list.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example usage:

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

```
local>show error ports 1-3

RX Frames                       TX Frames
---------------                 ----------------
CRC Error          0            Excessive Deferral      0
Undersize          0            CRC Error               0
Oversize           0            Late Collision          0
Fragment           0            Excessive Collision     0
Jabber       0                  Single Collision        0
Drop Pkts          0            Collision               0

local>
```

show utilization	
Purpose	Used to display real-time port utilization statistics.
Syntax	**show utilization**
Description	This command will display the real-time port utilization statistics for the switch.
Parameters	none.
Restrictions	none.

Example usage:

To display the port utilization statistics:

```
local>show utilization

Port    TX|sec     RX|sec     Util    Port    TX|sec     RX|sec     Util
----    ----------  ----------  ----    ----    ----------  ----------  ----
1:1          0           0          0    1:22         0           0          0
1:2          0           0          0    1:23         0           0          0
1:3          0           0          0    1:24         0           0          0
1:4          0           0          0    1:25         0           0          0
1:5          0           0          0    1:26        19          49          1
1:6          0           0          0    2:1          0           0          0
1:7          0           0          0    2:2          0           0          0
1:8          0           0          0    2:3          0           0          0
1:9          0           0          0    2:4          0           0          0
1:10         0           0          0    2:5          0           0          0
1:11         0           0          0    2:6          0           0          0
```

1:12	0	0	0	2:7	0	30	1
1:13	0	0	0	2:8	0	0	0
1:14	0	0	0	2:9	30	0	1
1:15	0	0	0	2:10	0	0	0
1:16	0	0	0	2:11	0	0	0
1:17	0	0	0	2:12	0	0	0
1:18	0	0	0	2:13	0	0	0
1:19	0	0	0	2:14	0	0	0
1:20	0	0	0	2:15	0	0	0
1:21	0	0	0	2:16	0	0	0

local>

clear counters	
Purpose	Used to clear the switch's statistics counters.
Syntax	**clear counters {ports <portlist>}**
Description	This command will clear the counters used by the switch to compile statistics.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear the counters:

```
local>clear counters ports 2:7-2:9
Command: clear counters ports 2:7-2:9
 Success.
local>
```

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

Example usage:

To clear the log information:

```
local>clear log
Command: clear log

 Success.

local>
```

show log	
Purpose	Used to display the switch history log.
Syntax	**show log {index <value>}**
Description	This command will display the contents of the switch's history log.
Parameters	index <value> – The show log command will display the history log until the log number reaches this value.
Restrictions	None.

Example usage:

To display the switch history log**:**

```
local>show log
Index Time      Log Text
----- ---------- ---------------------------------------------------------------
  4   000d00h50m Unit 1, Successful login through Console
(Username: Anonymous)
  3   000d00h50m Unit 1, Logout through Console (Username:
Anonymous)
  2   000d00h49m Unit 1, Successful login through Console
(Username: Anonymous)
000d00h49m Unit 1, Logout through Console (Username:
Anonymous)


local>
```

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

Example usage:

To the syslog function on the switch:

```
local>enable syslog
Command: enable syslog

 Success.

local>
```

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

Example usage:

To disable the syslog function on the swtich:

```
local>disable syslog
Command: disable syslog

 Success.

local>
```

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

Example usage:

To display the current status of the syslog function:

```
local>show syslog
Command: show syslog

 Syslog Global State: Enabled

local>
```

create syslog host	
Purpose	Used to create a new syslog 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[enabled|disabled]**
Description	The **create syslog host** command is used to create a new syslog host.
Parameters	all – Specifies that the command will be applied to all hosts. <index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. severity – Severity level indicator. These are described in the following: Bold font indicates that the corresponding severity level is currently supported on the switch. Numerical Code – Severity 0 Emergency: system is unusable 1 Alert: action must be taken immediately 2 Critical: critical conditions 3 Error: error conditions **4 Warning: warning conditions** 5 Notice: normal but significant condition **6 Informational: informational messages**

create syslog host

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 means the facility values the switch supports now.

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security|authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem

create syslog host

8	UUCP subsystem
9	clock daemon
10	security|authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	**local use 0 (local0)**
17	**local use 1 (local1)**
18	**local use 2 (local2)**
19	**local use 3 (local3)**
20	**local use 4 (local4)**
21	**local use 5 (local5)**
22	**local use 6 (local6)**
23	**local use 7 (local7)**

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

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

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

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

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

Example usage:

To create syslog host:

```
local>create syslog host 1 severity all facility local0

Command: create syslog host 1 severity all facility local0

 Success.

local>
```

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[enabled|disabled]**
Description	The **config syslog host** command is used to configure the syslog protocol to send system log information to a remote host.
Parameters	all – Specifies that the command will be applied to all hosts. <index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. severity – Severity level indicator. These are described in the following: Bold font indicates that the corresponding severity level is currently supported on the switch. Numerical Code – Severity 0 Emergency: system is unusable 1 Alert: action must be taken immediately 2 Critical: critical conditions 3 Error: error conditions **4 Warning: warning conditions**

config syslog host

5 Notice: normal but significant condition

6 Informational: informational messages

7 Debug: debug-level messages

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

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

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

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

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security|authorization messages
5	messages generated internally by syslog

config syslog host

6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security|authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	**local use 0 (local0)**
17	**local use 1 (local1)**
18	**local use 2 (local2)**
19	**local use 3 (local3)**
20	**local use 4 (local4)**
21	**local use 5 (local5)**
22	**local use 6 (local6)**
23	**local use 7 (local7)**

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

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

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

local3 – Specifies that local use 3 messages will

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

Example usage:

To configure a syslog host:

```
local>config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0
 Success.
local>
```

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

Example usage:

To delete a previously configured syslog host:

```
local>delete syslog host 4
Command: delete syslog host 4

 Success.

local>
```

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

Example usage:

To show Syslog host information:

```
local>show syslog host

Command: show syslog host

 Syslog Global State: Disabled

 Host Id  Host IP Address  Severiry   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

local>
```

11

SPANNING TREE COMMANDS

The switch supports 802.1d STP and 802.1w Rapid STP. The spanning tree commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config stp	maxage <value 6-40> hellotime <value 1-10> forwarddelay <value 4-30> priority <value 0-61440> fbpdu [enabled|disabled] version [rstp|stp] txholdcount <value 1-10>
config stp ports	<portlist> cost [auto|<value 1-200000000>] priority <value 0-240> migrate [yes|no] edge [true|false] p2p [true|false|auto] state [enabled|disabled]

Command	Parameters
enable stp	
disable stp	
show stp	
show stp ports	<portlist>

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

config stp	
Purpose	Used to setup STP and RSTP on the switch.
Syntax	**config stp {maxage <value 6-40> |hellotime <value 1-10> |forwarddelay <value 4-30>|priority <value 0-61440> |fbpdu [enabled|disabled]| txholdcount <value 1-10>| version[rstp|stp]}**
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch.
Parameters	maxage <value 6-40> – The maximum amount of time (in seconds) that the switch will wait to receive a BPDU packet before reconfiguring STP. The default is 20 seconds. hellotime <value 1-10> – The time interval between transmission of configuration messages by the root device. The default is 2 seconds. forwarddelay <value 4-30> – The maximum amount of time (in seconds) that the root device will wait before changing states. The default is 15 seconds. priority <value 0-61440> – A numerical value between 0 and 61440 that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device. The lower the numerical value, the higher the priority. The default is 32,768. fbpdu [enabled|disabled] – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the switch. The default is enabled. txholdcount <value 1-10> – the maximum

config stp	
	number of Hello packets transmitted per interval. Default value = 3. version [rstp|stp] – select the Spanning Tree Protocol version used for the switch. For IEEE 802.1d STP select stp. Select rstp for IEEE 802.1w Rapid STP.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure STP with maxage 18 and hellotime 4:

```
local>config stp maxage 18 hellotime 4
Command: config stp maxage 18 hellotime 4

 Success.

local>
```

config stp ports	
Purpose	Used to setup STP on the port level.
Syntax	**config stp ports <portlist> {cost [auto|<value 1-200000000>]|priority <value 0-240>| migrate [yes|no]| edge [true|false]| p2p [true|false|auto]| state [enabled|disabled]**
Description	This command is used to create and configure STP for a group of ports.
Parameters	Cost <value 1-200000000> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set from 1 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets. Default port cost: 100Mbps port = 200000 Gigabit port = 20000 priority <value 0-240> – Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port. Default = 128. <portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. migrate [yes|no] – yes will enable the port to

config stp ports	
	migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment. edge [true|false] – true designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. False indicates the port does not have edge port status. p2p [true|false|auto] – true indicates a point-to-point (p2p) shared link. These 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. state [enabled|disabled] – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure STP with path cost 19, priority 15, and state enabled for ports 1-5.

```
local>config stp_ports 1-5 cost 19 priority 15 state enabled
Command: config stp_ports 1-5 cost 19 priority 15 state enabled
 Success.
local>
```

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

Example Usage:

To enable STP, globally, on the switch:

```
local>enable stp
Command: enable stp
 Success.
local>
```

disable stp	
Purpose	Used to globally disable STP on the switch.
Syntax	**disable stp**
Description	This command allows the Spanning Tree Protocol to be globally disabled on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable STP on the switch:

```
local>disable stp
Command: disable stp
 Success.
local>
```

show stp

Purpose	Used to display the switch's current STP configuration.
Syntax	**show stp**
Description	This command displays the switch's current STP configuration.
Parameters	none
Restrictions	none.

Example Usage:

To display the status of STP on the switch:

Status 1: STP Enabled

```
local>show stp
Command: show stp

STP Status              : Enabled
Max Age                 : 20
Hello Time              : 2
Forward Delay           : 15
Priority                : 32768
STP Version             : RSTP
TX Hold Count           : 3
Forwarding BPDU         : Enabled
 Designated Root Bridge: 00-80-00-00-01-02
```

```
Root Priority              : 32767
Cost to Root               : 200015
Root Port                  : 2
Last Topology Change  : 77sec
Topology Changes Count: 198
Protocol Specification   : 3
Max Age                    : 20
Hello Time                 : 2
Forward Delay              : 15
Hold Time                  : 3
```

Status 2: STP Disabled

```
local>show stp
Command: show stp

STP Status           : Disabled
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15
Priority             : 32768
STP Version          : RSTP
TX Hold Count        : 3
Forwarding BPDU      : Enabled
```

```
local>
```

show stp ports	
Purpose	Used to display the switch's current per-port group STP configuration.
Syntax	**show stp ports <portlist>**
Description	This command displays the switch's current per-port group STP configuration.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies switch number 2, port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None

Example Usage:

To display the STP state of ports 1-9:

```
local>show stp ports 1-9
Command: show stp ports 1-9

Port   Designated Bridge   State   Cost      Pri   Edge  P2P Status      Role
------ ------------------- ------- --------- ----- ----- ----- --------- ------------
1      8000|000104031001   Yes   *200000   128   No    Yes   Forwarding  Designated
2            N|A           Yes   *200000   128   No    Yes   Disabled    Disabled
```

```
3              N|A              Yes  *200000  128  No    Yes  Disabled    Disabled

4              N|A              Yes  *200000  128  No    Yes  Disabled    Disabled
5              N|A              Yes  *200000  128  No    Yes  Disabled    Disabled

6              N|A              Yes  *200000  128  No    Yes  Disabled    Disabled
7       8000|000102030400       Yes   *200000  128  No    Yes  Forwarding Root
8              N|A              Yes  *200000  128  No    Yes  Disabled    Disabled
9              N|A              Yes  *200000  128  No    Yes  Disabled    Disabled

local>
```

12

LAYER 2 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>
delete fdb	<vlan_name 32> <macaddr> [add|delete] <portlist>
clear fdb	vlan <vlan_name 32> port <port>|all

Command	Parameters
show multicast_fdb	vlan <vlan_name 32> mac_address <macaddr>
config fdb aging_time	<sec 10-1000000>
show fdb	port <port> vlan <vlan_name 32> mac_address <macaddr> static aging_time

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

create fdb	
Purpose	Used to create a static entry to the unicast MAC address forwarding table (database)
Syntax	**create fdb <vlan_name32> <macaddr> [port <port>]**
Description	This command will make an entry into the switch's unicast MAC address forwarding database.
Parameters	<vlan_name 32> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table. <port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an unicast MAC forwarding**:**

```
local>create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5
 Success.
local>
```

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

Example Usage:

To create multicast MAC forwarding:

```
local>create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00
 Success.
local>
```

config multicast_fdb	
Purpose	Used to configure the switch's multicast MAC address forwarding database.
Syntax	**config multicast_fdb <vlan_name 32> <macaddr> [add|delete] [egress|forbidden] <portlist>**
Description	This command configures the multicast MAC address forwarding table.
Parameters	<vlan_name 32> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table. [add|delete] – Add will add the MAC address to the forwarding table, delete will remove the MAC address from the forwarding table. [egress|forbidden] – Egress specifies the port as being a source of multicast packets originating from the MAC address specified above, forbidden specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. <portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add multicast MAC forwarding:

```
local>config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Success.
local>
```

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

Example Usage:

To delete a permanent FDB entry:

```
local>delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02
 Success.
local>
```

clear fdb	
Purpose	Used to clear the switch's forwarding database of all dynamically learned MAC addresses.
Syntax	**clear fdb [vlan <vlan_name 32>|port <port>|all]**
Description	This command is used to clear dynamically learned entries to the switch's forwarding database.
Parameters	<vlan_name 32> – The name of the VLAN on which the MAC address resides. <port> – 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:

```
local>clear fdb all
Command: clear fdb all
 Success.
local>
```

show multicast_fdb	
Purpose	Used to display the contents of the switch's multicast forwarding database.
Syntax	**show multicast_fdb [vlan <vlan_name 32>|mac_address <macaddr>**
Description	This command is used to display the current contents of the switch's multicast MAC address forwarding database.
Parameters	<vlan_name 32> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table.
Restrictions	none.

Example Usage:

To display multicast MAC address table:

```
local>show multicast_fdb
Command: show multicast_fdb
 VLAN Name       : default
 MAC Address     : 01-00-5E-00-00-00
 Egress Ports    : 1-5, 26
 Mode            : Static

 Total Entries   : 1
local>
```

config fdb aging_time	
Purpose	Used to set the aging time of the forwarding database.
Syntax	**config fdb aging_time <sec 10-100000>**
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 1,000,000 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> – The aging time for the MAC address forwarding database value.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set the fdb aging time:

```
local>config fdb aging_time 25
Command: config fdb aging_time 25
 Success.
local>
```

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

Example Usage:

To display unicast MAC address table:

```
local>show fdb
Command: show fdb

 Unicast MAC Address Ageing Time  = 300

 VID   VLAN Name      MAC Address          Port    Type
 ----  ----------     -------------------  ------  ---------
 1     default        00-00-00-00-01-01    7       Dynamic
 1     default        00-00-00-00-01-02    7       Dynamic
 1     default        00-50-BA-6B-2A-29    7       Dynamic

 Total Entries = 3

local>
```

13

TRAFFIC CONTROL COMMANDS

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

Command	Parameters
config traffic control	<storm_grouplist 1-8> all broadcast [enabled|disabled] multicast [enabled|disabled] dlf [enabled|disabled] threshold <value 0-255>
show traffic control	group_list <storm_grouplist 1-8>

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

config traffic control	
Purpose	Used to configure broadcast|multicast traffic control.
Syntax	**config traffic control [<storm_grouplist 1-8>|all] broadcast [enabled|disabled]|multicast [enabled|disabled]|dlf [enabled|disabled]|threshold <value 0-255>**
Description	This command is used to configure broadcast storm control.
Parameters	<storm_grouplist 1-8> – Used to specify a broadcast storm control group with the syntax: module_id:group_id. all – Specifies all broadcast storm control groups on the switch. broadcast [enabled|disabled] – Enables or disables broadcast storm control. multicast [enabled|disabled] – Enables or disables multicast storm control. dlf [enabled|disabled] – Enables or disables dlf traffic control. threshold <value 0-255> – The upper threshold at which the specified traffic control is switched on. The <value 0-255> is the number of broadcast|multicast|dlf packets, in Kbps, received by the switch that will trigger the storm traffic control measures.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure traffic control and state:

```
local>config traffic control 1-3,1-2 broadcast enabled
Command: config traffic control 1-3 broadcast enabled

 Success.

local>
```

show traffic control	
Purpose	Used to display current traffic control settings.
Syntax	**show traffic control <storm_grouplist 1-8>**
Description	This command displays the current storm traffic control configuration on the switch.
Parameters	group_list <storm_grouplist 1-8> – Used to specify a broadcast storm control group with the syntax: module_id:group_id.
Restrictions	none.

Example Usage:

To display traffic control setting:

local>show traffic control

Command: show traffic control

Traffic Control

Group [ports]	Threshold	Broadcast Storm	Multicast Storm	Destination Lookup Fail
1 [1 - 8]	128	Enabled	Disabled	Disabled
2 [9 - 16]	128	Enabled	Disabled	Disabled
3 [17 - 24]	128	Enabled	Disabled	Disabled
4 [25 - 32]	128	Disabled	Disabled	Disabled
5 [33 - 40]	128	Disabled	Disabled	Disabled
6 [41 - 48]	128	Enabled	Disabled	Disabled
7 [49]	128	Enabled	Disabled	Disabled
8 [50]	128	Disabled	Disabled	Disabled

Total Entries: 8

14

QOS COMMANDS

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

Command	Parameters
config scheduling	<class_id 0-3> mac_packet <value 0-255> max_latency <value 0-255>
show scheduling	
config 802.1p user_priority	<priority 0-7> <class_id 0-3>
show 802.1p user_priority	
config 802.1p default_priority	<portlist> all <priority 0-7>
show 802.1p default_priority	all <portlist>
config traffic_segmentation	<portlist> forward_list [null | <portlist>]

Command	Parameters
show traffic_segmentation	<portlist>
config bandwidth_control	<portlist> rx_rate no_limit <value 1-1000> tx_rate no_limit <value 1-1000>
show bandwidth_control	<portlist>

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

config scheduling

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

config scheduling

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

config scheduling	
	packets. A value between 0 and 255 can be specified – with this value multiplied by 16 ms to arrive at the total allowed time for the queue to transmit packets. For example, a value of 3 specifies 3 X 16 = 48 ms. The queue will continue transmitting the last packet until it is finished when the max_latency timer expires.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

```
local>config scheduling 0 max_packet 100 max_latency 150
Command: config scheduling 0 max_packet 100 max_latency 150
 Success.
local>
```

show scheduling	
Purpose	Used to display the current traffic scheduling mechanisms in use on the switch.
Syntax	**show scheduling**
Description	This command will display the current traffic scheduling mechanisms in use on the switch.
Parameters	none.
Restrictions	none.

Example Usage:

```
local> show scheduling
Command: show scheduling
QOS Output Scheduling
      MAX. Packets  MAX. Latency
      ------------  ------------
Class-0    100          150
Class-1     99          100
Class-2     91          101
Class-3     21          201

local>
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the four hardware queues available on the switch.
Syntax	**config 802.1p user_priority <priority 0-7> <class_id 0-3>**
Description	This command allows you to configure the way the switch will map an incoming packet, based on its 802.1p user priority, to one of the four available hardware priority queues on the switch. The switch's default is to map the following incoming 802.1p user priority values to the four hardware priority queues: 802.1p — Hardware Queue — Remark 0 — 1 — Mid-low 1 — 0 — Lowest 2 — 0 — Lowest 3 — 1 — Mid-low 4 — 2 — Mid-high 5 — 2 — Mid-high 6 — 3 — Highest 7 — 3 — Highest. This mapping scheme is based upon recommendations contained in IEEE 802.1D. You can change this mapping by specifying the 802.1p user priority you want to go to the <class_id 0-3> (the number of the hardware queue). <priority 0-7> – The 802.1p user priority you want to associate with the <class_id 0-3> (the number of the hardware queue) with.

config 802.1p user_priority	
	<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:

```
local> config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3
 Success.
local>
```

show 802.1p user_priority	
Purpose	Used to display the current 802.1p user priority to hardware priority queue mapping in use by the switch.
Syntax	**show 802.1p user_priority**
Description	This command will display the current 802.1p user priority to hardware priority queue mapping in use by the switch.
Parameters	None.
Restrictions	None.

Example Usage:

```
local> show 802.1p user_priority
Command: show 802.1p user_priority
QOS Class of Traffic
Priority-0  ->  <Class-1>
Priority-1  ->  <Class-3>
Priority-2  ->  <Class-0>
Priority-3  ->  <Class-1>
Priority-4  ->  <Class-2>
Priority-5  ->  <Class-2>
Priority-6  ->  <Class-3>
Priority-7  ->  <Class-3>
local>
```

config 802.1p default_priority	
Purpose	Used to configure the 802.1p default priority settings on the switch. If an untagged packet is received by the switch, the priority configured with this command will be written to the packet's priority field.
Syntax	**config 802.1p default_priority [<portlist>|all] <priority 0-7>**
Description	This command allows you to specify default priority handling of untagged packets received by the switch. The priority value entered with this command will be used to determine which of the four hardware priority queues the packet is forwarded to.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies that the command applies to all ports on the switch (or in the switch stack). <priority 0-7> – The priority value you want to assign to untagged packets received by the switch or a range of ports on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

```
local> config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5
Success.
local>
```

show 802.1p default_priority	
Purpose	Used to display the current default priority settings on the switch.
Syntax	**show 802.1p default_priority**
Description	This command is used to display the current default priority settings on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

```
local> show 802.1p default_priority all
Command: show 802.1p default_priority

Port    Priority
-------  -----------
1        0
2        0
3        0
4        0
5        0
6        0
7        0
8        0
9        0
```

```
10      0
11      0
12      0
13      0
14      0
15      0
16      0
17      0
18      0
19      0
20      0
CTRL+C ESC q QUIT SPACE n Next Page Enter Next Entry a All
```

config traffic_segmentation

Purpose	Used to configure traffic segmentation on the switch.
Syntax	**config traffic_segmentation <portlist> forward_list [null|<portlist>]**
Description	The config traffic_segmentation command is used to configure traffic segmentation on the switch.
Parameters	<portlist> – Specifies a range of ports that will be configured for traffic segmentation. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. forward_list – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist above. null – Specifies that packets cannot be forwarded to any ports. <portlist> – Specifies a range of ports that will be configured for traffic segmentation. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
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:

```
local> config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15
Success.
local>
```

show traffic_segmentation	
Purpose	Used to display the current traffic segmentation configuration on the switch.
Syntax	**show traffic_segmentation <portlist>**
Description	The show traffic_segmentation command is used to display the current traffic segmentation configuration on the switch.
Parameters	<portlist> – Specifies a range of ports for which the current traffic segmentation configuration on the switch will be displayed. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display the current traffic segmentation configuration on the switch:

```
local> show traffic_segmentation
Command: show traffic_segmentation
Traffic Segmentation Table

Port  Forward Portlist
----  -------------------------------------------------
1     9-15
```

```
2    9-15
3    9-15
4    9-15
5    9-15
6    9-15
7    9-15
8    9-15
9    9-15
10   9-15
11   1-26
12   1-26
13   1-26
14   1-26
15   1-26
16   1-26
17   1-26
18   1-26
CTRL+C ESC q QUIT SPACE n Next Page Enter Next Entry a All
```

config bandwidth_control	
Purpose	Used to configure bandwidth control on a by-port basis.
Syntax	**config bandwidth_control <portlist> {rx rate [no_limit|<value 1-1000>]|tx_rate [no_limit|<value 1-1000>]}**
Description	The config bandwidth_control command is used to configure bandwidth on a by-port basis.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. rx_rate – Specifies that one of the parameters below (no_limit or <value 1-1000**>**) will be applied to the rate at which the above specified ports will be allowed to receive packets no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports. <value 1-1000> – Specifies the limit, in Mbps, that the above ports will be allowed to receive packets. tx_rate – Specifies that one of the parameters below (no_limit or <value 1-1000**>**) will be applied to the rate at which the above specified ports will be allowed to transmit packets. no_limit – Specifies that there will be no limit on the rate of packets received by the above

config bandwidth_control	
	specified ports. <value 1-1000> – Specifies the limit, in Mbps, that the above ports will be allowed to receive packets.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure bandwidth control:

```
local>config bandwidth_control 1-10 tx_rate 10
Command: config bandwidth_control 1-10 tx_rate 10
 Success.
local>
```

show bandwidth_control	
Purpose	Used to display the bandwidth control configuration on the switch.
Syntax	**show bandwidth_control {<portlist>}**
Description	The show bandwidth_control command displays the current bandwidth control configuration on the switch, on a port-by-port basis.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To show bandwidth control for ports 1 through 11:

```
local>show bandwidth_control  1-11
Command: show bandwidth_control 1-11
Bandwidth Control Table
Port    RX Rate (Mbit|sec)    TX_RATE (Mbit|sec)
----    ----------------------    ---------------------
1       no_limit              10
2       no_limit              10
3       no_limit              10
```

```
4       no_limit            10
5       no_limit            10
6       no_limit            10
7       no_limit            10
8       no_limit            10
9       no_limit            10
10      no_limit            10
11      no_limit            no_limit

local>
```

15

PORT MIRRORING COMMANDS

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

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

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

config mirror port	
Purpose	Used to configure a mirror port – source port pair on the switch.
Syntax	**config mirror port <port> add source ports <portlist> [rx|tx|both]**
Description	This command allows you to add or delete mirroring ports. It also allows a range of ports to have all of their traffic sent to a designated port – where a network sniffer or other device can monitor the network traffic. You can also specify that only traffic received by or sent by or both is mirrored to the Target port.
Parameters	<port> – This specifies the Target port (the port where mirrored packets will be sent). <portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list. tx – Allows the mirroring of only packets sent (flowing out of) the port or ports in the port list. both – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add the mirroring ports:

```
local> config mirror port 5 add source ports 1-4 both
Command: config mirror port 5 add source ports 1-4 both

 Success.

local>
```

enable mirror	
Purpose	Used to enable a previously entered port mirroring configuration.
Syntax	**enable mirror**
Description	This command, combined with the disable mirror command below, allows you to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	none.
Restrictions	none.

Example Usage:

To enable mirroring configurations:

```
local>enable mirror
Command: enable mirror

 Success.

local>
```

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

Example Usage:

To disable mirroring configurations:

```
local>disable mirror
Command: disable mirror

 Success.

local>
```

show mirror	
Purpose	Used to show the current port mirroring configuration on the switch.
Syntax	**show mirror**
Description	This command displays the current port mirroring configuration on the switch.
Parameters	None
Restrictions	none.

Example Usage:

To display mirroring configuration:

```
local>show mirror
Command: show mirror
 Current Settings
 Mirror Status: Enabled
 Target Port   : 9
 Mirrored Port
            RX:
            TX: 1-5
local>
```

16

VLAN COMMANDS

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

Command	Parameters
create vlan	<vlan_name 32> tag <vlanid> advertisement
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> add [tagged|untagged|forbidden] <portlist>
config vlan	<vlan_name 32> delete <portlist>
config vlan	<vlan_name 32> advertisement [enabled|disabled]
config gvrp	<portlist> all state [enabled|disabled] ingress_checking [enabled|disabled]

Command	Parameters
	pvid <vlanid 1-4094>
enable gvrp	
disable gvrp	
show vlan	<vlan_name 32>
show gvrp	<portlist>

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

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

Example Usage:

To create a VLAN v1, tag 2:

```
local>create vlan v1 tag 2
Command: create vlan v1 tag 2
 Success.

local>
```

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

Example Usage:

To remove a vlan v1:

```
local>delete vlan v1
Command: delete vlan v1

 Success.

local>
```

config vlan add	
Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan <vlan_name 32> add [tagged|untagged|forbidden] <portlist>**
Description	This command allows you to add ports to the port list of a previously configured VLAN. You can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	<vlan_name 32> – The name of the VLAN you want to add ports to. tagged – Specifies the additional ports as tagged. untagged – Specifies the additional ports as untagged. forbidden – Specifies the additional ports as forbidden. <portlist> – A range of ports to add to the VLAN. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

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

 Success.

local>
```

config vlan delete	
Purpose	Used to delete one or more ports from a previously configured VLAN.
Syntax	**config vlan <vlan_name 32> delete <portlist>**
Description	This command allows you to delete ports from a previously configured VLAN's port list.
Parameters	<vlan_name 32> – The name of the VLAN you want to delete ports from. <portlist> – A range of ports you want to delete from the above specified VLAN. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete 4 through 8 to the VLAN v1:

```
local>config vlan v1 delete 4-8
Command: config vlan v1 delete 4-8
 Success.
local>
```

config vlan advertisement	
Purpose	Used to enable or disable the VLAN advertisement.
Syntax	**config vlan <vlan_name> advertisement [enabled|disabled]**
Description	This command is used to enable or disable GVRP on the specified VLAN.
Parameters	<vlan_name 32> – The name of the VLAN on which you want to enable or disable GVRP. enabled – Enables GVRP on the specified VLAN. disabled – Disables GVRP on the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable the VLAN default advertisement:

```
local>config vlan default advertisement enabled
Command: config vlan default advertisement enabled
 Success.
local>
```

config gvrp	
Purpose	Used to configure GVRP on the switch.
Syntax	**config gvrp [<portlist>|all] {state [enabled|disabled]|ingress_checking [enabled|disabled] pvid <vlanid 1-4096> }**
Description	This command is used to configure the Group VLAN Registration Protocol on the switch. You can configure ingress checking and the sending and receiving of GVRP information.
Parameters	<portlist> – A range of ports for which you want ingress checking. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch. state [enabled|disabled] – Enabled or disables GVRP for the ports specified in the port list. ingress_checking [enabled|disabled] – Enables or disables ingress checking for the specified port list. pvid <vlanid 1-4094> – This is the VLAN ID (VID) of the VLAN for which you want to configure GVRP.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
local>config gvrp 1-5 state enabled ingress_checking enabled
Command: config gvrp 1-5 state enabled ingress_checking
enabled

 Success.

local>
```

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

Example Usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
local>enable gvrp
Command: enable gvrp

 Success.

local>
```

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

Example Usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
local>disable gvrp
Command: disable gvrp

 Success.

local>
```

show vlan	
Purpose	Used to display the current VLAN configuration on the switch
Syntax	**show vlan {<vlan_name 32>}**
Description	This command displays summary information about each VLAN including the VLAN ID, VLAN name, the Tagging|Untagging status, and the Member|Non-member|Forbidden status of each port that is a member of the VLAN.
Parameters	<vlan_name 32> – The VLAN name of the VLAN for which you want to display a summary of settings.
Restrictions	none.

Example Usage:

To display VLAN settings:

```
local>show vlan
Command: show vlan
VID           : 1          VLAN Name     : default
VLAN TYPE     : static     Advertisement : Enabled
Member ports  : 1-50
 Static ports : 1-50
Untagged ports : 1-50
Forbidden ports :
 Total Entries : 1
local>
```

show gvrp	
Purpose	Used to display the GVRP status for a port list on the switch.
Syntax	**show gvrp {<portlist>}**
Description	This command displays the GVRP status for a port list on the switch, including the PVID. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If a packet is received by the port, and Ingress Checking is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive and forward the packet.
Parameters	<portlist> – A range of ports for which you want ingress checking. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	none.

Example Usage:

To display 802.1Q port setting:

```
local> show gvrp
Command: show gvrp
 Global GVRP : Disabled
 Port   PVID    GVRP        Ingress Checking
 ----   ------- --------    -------------------
 1      21      Enabled         Enabled
 2      21      Enabled         Enabled
 3      21      Enabled         Enabled
 4      21      Enabled         Enabled
 5      21      Enabled         Enabled
 6      1       Disabled        Disabled
 7      1       Disabled        Disabled
 8      1       Disabled        Disabled
 9      1       Disabled        Disabled
 10     1       Disabled        Disabled
 11     1       Disabled        Disabled
 12     1       Disabled        Disabled
 13     1       Disabled        Disabled
 14     1       Disabled        Disabled
 15     1       Disabled        Disabled
 16     1       Disabled        Disabled
 17     1       Disabled        Disabled
 18     1       Disabled        Disabled
CTRL+C ESC q QUIT SPACE n Next Page Enter Next Entry a All
```

17

ASYMMETRIC VLAN COMMANDS

The DES-3250TG automatically implements Asymmetric VLANs system wide. Asymmetric VLANs are used to segment the network to allow all ports to forward packets to the default VLAN while creating a unique PVID for each to allow forwarding from the default VLAN to each port. This arrangement is a convenient method to quickly setup an environment that allows access to shared resources suchs as servers or gateway routers (via the default VLAN). Workstations are able to forward traffic to the default VLAN but are unaware of other existing VLANs. The default VLAN is able to forward to all ports. Therefore when Asymmetric VLANs are enabled, forwarding between participating ports must be done via a shared resource on the default VLAN.

This feature can be enabled with the following important restrictions:

- Each participating port must be untagged.
- GVRP and IGMP Snooping is not supported

Command	Parameters
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	

enable asymmetric_vlan	
Purpose	Used to enable Asymmetric VLANs system wide.
Syntax	**enable asymmetric_vlan**
Description	This command enables Asymmetric VLANs system wide. A unique PVID is assigned to all ports creating a separate VLAN for each port. Each port is still able to receive frames from the defult VLAN. Asymmetric VLANs are disabled by default.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable Asymmetric VLANs:

```
local>enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

local>
```

disable asymmetric_vlan	
Purpose	Used to disable Assymetric VLANs system wide.
Syntax	**disable asymmetric_vlan**
Description	This will disable Assymetric VLANs configured on the system. By default, Asymmetric VLANs are diabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable Asymmetric VLANs:

```
local>disable asymmetric_vlan

Command: disable asymmetric_vlan

VLAN setting will be reset to default value.  Are you sure you want
to proceed with asymmetric vlan disable? (y/n)y

Success.


local>
```

show asymmetric_vlan	
Purpose	Used to display Asymmetric VLAN status for the system.
Syntax	**show asymmetric_vlan**
Description	This displays whether Asymmetric VLANs are enable or disabled system wide.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display Asymmetric VLANs status:

```
local>show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric Vlan : Enabled

local>
```

18

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <group_id 1-6> {type[lacp|static]}
delete link_aggregation	group_id <group_id 1-6>
config link_aggregation	group_id <group_id 1-6> master_port <port> ports <portlist> state [enabled|disabled]
config link_aggregation algorithm	mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest
show link_aggregation	group_id <group_id 1-6>

Command	Parameters
	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 group _id	
Purpose	Used to create a link aggregation group on the switch.
Syntax	**create link_aggregation group_id <group_id 1-6> {type[lacp|static]}**
Description	This command will create a link aggregation group with a unique indentifier.
Parameters	<group_id 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. type – Specify the type of link aggregagation used for the group. If type is not specified the default type is static. lacp – This designates the port group as LACP compliant. LACP compliant ports may be further configured (see config lacp_ports). static – This designates the port group as a static trunk group. Static trunk groups can not be changed as easily as LACP compliant port groups since both devices connected to the trunked group must be manually configured if the configuration of the trunked group is changed.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create link aggregation group:

```
local>create link_aggregation group_id 1
Command: create link_aggregation group_id 1

 Success.

local>
```

delete link_aggregation group_id	
Purpose	Used to delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <group_id 1-6>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<group_id 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:

```
local>delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

 Success.

local>
```

config link_aggregation	
Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <group_id 1-6> {master_port <port>|ports <portlist>| state [enabled|disabled]**
Description	This command allows you to configure a link aggregation group that was created with the **create link_aggregation** command above.
Parameters	<group_id 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. <port> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. <portlist> – A range of ports for which you want ingress checking. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command. Link aggregation groups may not overlap and must be contained on a single switch.

Example usage:

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

```
local>config link_aggregation group_id 1 master_port 5 ports 5-7,9
Command: config link_aggregation group_id 1 master_port 5 ports 5-7,9

Success.

local>
```

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

Example usage:

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

```
local>config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

 Success.

local>
```

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

Example usage:

To display Link Aggregation configuration

```
local>show link_aggregation
Command: show link_aggregation
Link Aggregation Algorithm = MAC-source
Group ID          : 1
Type              : LACP
Master Port       : 4
Member Port       : 3-4
Active Port       :
Status            : Enabled
Flooding Port     : 4
```

config lacp_port	
Purpose	Used to configure the Link Aggregation Control Protocol (LACP) on a per-port basis.
Syntax	**config lacp_ports <portlist> mode [active|passive]**
Description	Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer.
Parameters	<portlist> – mode – active passive
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure ports 1 through 5 as being LACP active:

```
local>config lacp_port 1-5 mode active
Command: config lacp_port 1-5 mode active


local>
```

show lacp_ports	
Purpose	Used to display the current status of LACP on a per-port basis.
Syntax	**show lacp_port {<portlist>}**
Description	Displays the current status of LACP on a per-port basis.
Parameters	<portlist> – A range of ports for which you want ingress checking. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the LACP status of ports 1 through 5:

```
local>show lacp_port 1-5
Command: show lacp_port 1-5
Port   Activity
------ ---------
1      Active
2      Active
3      Active
4      Passive
5      Passive
local>
```

19

IP INTERFACE 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	vlan <vlan_name 32> ipaddress <network_address> state [enabled|disabled] bootp dhcp
show ipif	

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

config ipif System	
Purpose	Used to configure the System IP interface.
Syntax	**config ipif System [{vlan <vlan_name 32>|ipaddress <network_address>|state [enabled|disabled]|bootp|dhcp}]**
Description	This command is used to configure the System IP interface on the switch.
Parameters	<vlan_name 32> – The name of the VLAN corresponding to the System IP interface. <network_address> – IP address and netmask of the IP interface to be created. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16). state [enabled|disabled] – Allows you to enable or disable the IP interface. bootp – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface. dhcp – Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System IP interface.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the IP interface System:

```
local>config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

 Success.

local>
```

show ipif	
Purpose	Used to display the configuration of an IP interface on the switch.
Syntax	**show ipif**
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:

```
local>show ipif
Command: show ipif

 IP Interface Settings
 Interface Name : System
 IP Address     : 10.90.90.90    (MANUAL)
 Subnet Mask    : 255.0.0.0
 VLAN Name      : default
 Admin. State   : Disabled
 Member Ports   : 1-50

Total Entries   :  1
local>
```

20

IGMP SNOOPING 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 igmp_snooping	<vlan_name 32> all host_timeout <sec 1-16711450> router_timeout <sec 1-16711450> leave_timer <sec 1-16711450> state [enabled|disabled]
config igmp_snooping querier	<vlan_name 32> all query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enabled|disabled]
config router_ports	<vlan_name 32> [add|delete] <portlist>

Command	Parameters
enable igmp snopping	forward-mcrouter-only
show igmp snooping	vlan <vlan_name 32>
show igmp snooping group	vlan <vlan_name 32>
show router ports	vlan <vlan_name 32> static dynamic

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

config igmp_snooping	
Purpose	Used to configure IGMP snooping on the switch.
Syntax	**config igmp_snooping [<vlan_name>|all] {host_timeout <sec>|router_timeout <sec>|leave_timer <sec>|state [enabled|disabled]}**
Description	This command allows you to configure IGMP snooping on the switch.
Parameters	<vlan_name> – The name of the VLAN for which IGMP snooping is to be configured. host_timeout <sec> – 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. route_timeout <sec> – Specifies the maximum amount of time a route will remain in the switch's can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds. leave_timer <sec> – Leave timer. The default is 2 seconds. state [enabled|disabled] – Allows you to enable or disable IGMP snooping for the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
local>config igmp_snooping default host_timeout 250 state
enabled
Command: config igmp_snooping default host_timeout 250 state
enabled

 Success.

local>
```

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, the permitted packet loss that guarantees IGMP snooping.
Syntax	**config igmp_snooping querier [<vlan_name>|all] {query_interval <sec>|max_response_time <sec>|robustness_variable <value>|last_member_query_interval <sec>|state [enabled|disabled]**
Description	This command configures IGMP snooping querier.
Parameters	<vlan_name> – The name of the VLAN for which IGMP snooping querier is to be configured. query_interval <sec> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. max_response_time <sec> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds. robustness_variable <value> – 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

config igmp_snooping querier

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 <sec> – 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 [enabled|disabled] – Allows the switch to be specified as an IGMP Querier or Non-querier.

Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
local>config igmp_snooping querier default query_interval 125
state enabled

Command: config igmp_snooping querier default query_interval
125 state enabled

 Success.

local>
```

config router_ports	
Purpose	Used to configure ports as router ports.
Syntax	**config router_ports <vlan_name> [add|delete] <portlist>**
Description	This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	<vlan_name> – The name of the VLAN on which the router port resides. <portlist> – A range of ports for which you want ingress checking. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set up static router ports:

```
local>config router_ports default add 1-10
Command: config router_ports default add 1-10

 Success.

local>
```

enable igmp_snooping	
Purpose	Used to enable IGMP snooping on the switch.
Syntax	**enable igmp_snooping {forward-mcrouter-only}**
Description	This command allows you to enable IGMP snooping on the switch. If **forward-mcrouter-only** is specified, the switch will forward all multicast traffic to the multicast router, only. Otherwise, the switch forwards all mulitcast traffic to any IP router.
Parameters	forward_mcrouter_only – Specifies that the switch should forward all multicast traffic to a multicast-enabled router only. 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:

```
local>enable igmp_snooping
Command: enable igmp_snooping

 Success.


local>
```

disable igmp_snooping	
Purpose	Used to enable IGMP snooping on the switch.
Syntax	**disable igmp_snooping**
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	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable IGMP snooping on the switch:

```
local>disable igmp_snooping
Command: disable igmp_snooping

 Success.

local>
```

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

Example usage:

To show igmp snooping:

```
local>show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State    : Disabled
Multicast router Only         : Disabled
VLAN  Name                    : default
Query Interval                : 125
Max Response Time             : 10
Robustness Value              : 2
Last Member Query Interval    : 1
Host Timeout                  : 260
```

```
Route Timeout                    : 260
Leave Timer                      : 2
Querier State                    : Disabled
Querier Router Behavior          : Non-Querier
State                            : Disabled

VLAN  Name                       : vlan2
Query Interval                   : 125
Max Response Time                : 10
Robustness Value                 : 2
Last Member Query Interval       : 1
Host Timeout                     : 260
Route Timeout                    : 260
Leave Timer                      : 2
Querier State                    : Disabled
Querier Router Behavior          : Non-Querier
State                            : Disabled


Total Entries: 2

local>
```

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

Example usage:

To show igmp snooping group:

```
local>show igmp_snooping group
Command: show igmp_snooping group

VLAN Name      : default
Multicast group: 224.0.0.2
MAC address    : 01-00-5E-00-00-02
Reports        : 1
Port Member    : 26

VLAN Name      : default
Multicast group: 224.0.0.9
MAC address    : 01-00-5E-00-00-09
Reports        : 1
```

```
Port Member    : 26
VLAN Name      : default
Multicast group: 234.5.6.7
MAC address    : 01-00-5E-05-06-07
Reports        : 1
Port Member    : 26

VLAN Name      : default
Multicast group: 236.54.63.75
MAC address    : 01-00-5E-36-3F-4B
Reports        : 1
Port Member    : 26

VLAN Name      : default
Multicast group: 239.255.255.250
MAC address    : 01-00-5E-7F-FF-FA
Reports        : 2
Port Member    : 26

VLAN Name      : default
Multicast group: 239.255.255.254
MAC address    : 01-00-5E-7F-FF-FE
Reports        : 1
Port Member    : 26
Total Entries  : 6
local>
```

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

Example usage:

To display the router ports.

```
local>show router_ports
Command: show router_ports

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

  Total Entries: 1

local>
```

21

802.1X COMMANDS

The DES-3250TG implements the server-side of the IEEE 802.1x Port-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the switch that a user or network device must meet before allowing that port to forward or receive frames.

Command	Parameters
enable 802.1x	
disable 802.1x	
show 802.1x auth_configuration	ports <portlist>
show 802.1x auth_state	ports <portlist>
config 802.1x capability	ports <portlist>|all authenticator none
config 802.1x auth_parameter	ports <portlist>|all default direction [both|in] port_control [force_unauth|auto|force_auth]

Command	Parameters
	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 [enabled|disabled]
config 802.1x init	port_based ports [<portlist>|all]|mac_based ports [<portlist>|all]| {mac_address <macaddr>}
config 802.1x reauth	port_based ports [<portlist>|all]|mac_based ports [<portlist>|all]| {mac_address <macaddr>}
config 802.1x auth_mode	[port_based|mac_based]
config radius add	<server_index 1-3> <server_ip> key <passwd 32> default auth_port <udp_port_number> acct_port <udp_port_number>
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> ipaddress <server_ip> key <passwd 32> auth_port <udp_port_number> acct_port <udp_port_number>
show radius	

enable 802.1x	
Purpose	Used to enable the 802.1x server on the switch.
Syntax	**enable 802.1x**
Description	The enable 802.1x command enables the 802.1x Port-based Network Access control server application on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable 802.1x switch-wide:

```
local>enable 802.1x
Command: enable 802.1x

 Success.

local>
```

disable 802.1x	
Purpose	Used to disable the 802.1x server on the switch.
Syntax	**disable 802.1x**
Description	The disable 802.1x command is used to disable the 802.1x Port-based Network Access control server application on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable 802.1x on the switch:

```
local>disable 802.1x
Command: disable 802.1x

Success.

local>
```

show 802.1x auth_configuratic n	
Purpose	Used to display the current authenticated configuration of the 802.1x server on the switch.
Syntax	**show 802.1x auth_configuration {ports <portlist>}**
Description	The show 802.1x auth_configuration command is used to display the current authenticated configuration of the 802.1x Port-based Network Access Control server application on the switch.
Parameters	ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. The following details what is displayed: 802.1x Enabled|Disabled – Shows the current status of 802.1x functions on the switch. Authentication Mode: Port_based |Mac_based |None – Shows the current authentication mode. Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the switch and a Radius server. Port number – Shows the physical port number on the switch. Capability: Authenticator|None – Shows the capability of 802.1x functions on the port number displayed above. There are four 802.1x capabilities that can be set on the switch:

show 802.1x auth_configuratic n	
	Authenciator, Suplicant, Authenticator and Suplicant, and None. AdminCrlDir: Both|In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. OpenCtlDir: Both|In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. Port Control: ForceAuth|ForceUnauth|Auto – Shows the adminstrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized. QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt. TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request|Identity packets. SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request|Identity packets. ServerTimeout – Shows the length of time to wait for a response from a Radius server. MaxReq – Shows the maximum number of times to retry sending packets to the supplicant. ReAuthPeriod – shows the time interval

show 802.1x auth_configuratic n	
	between successive re-authentications. ReAuthenticate: Enabled|Disabled – Shows whether or not to re-authenticate.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display 802.1x authentication configuration port settings for port 1:

```
local>show 802.1x auth_configuration
Command: show 802.1x auth_configuration

  802.1X                      : Disabled
  Authentication Mode         : None
  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
```

```
local>
```

show 802.1x auth_state

Purpose	Used to display the current authentication state of the 802.1x server on the switch.
Syntax	**show 802.1x auth_state {ports <portlist>}**
Description	The show 802.1x auth_state command is used to display the current authentication state of the 802.1x Port-based Network Access Control server application on the switch.
Parameters	ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. The following details what is displayed: Port number – Shows the physical port number on the switch. Auth PAE State: Initalize|Disconnected|Connecting| Authenticating|Authenticated|Held |ForceAuth|ForceUnauth – Shows the current state of the Authenticator PAE. Backend State: Request|Response|Fail| Idle|Initalize|Success |Timeout – Shows the current state of the Backend Authenticator.

show 802.1x auth_state	
	Port Status: Authorized|Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display the 802.1x authentication state:

```
local>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
local>
```

config 802.1x capability	
Purpose	Used to configure the 802.1x capability of a range of ports on the switch.
Syntax	**config 802.1x capability ports [<portlist>|all] [authenticator|none]**
Description	The config 802.1x command has two capabilities that can be set for each port: Authenticator and None.
Parameters	<portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch. authenticator – A user must pass the authentication process to gain access to the network. none – The port is not controlled by the 802.1x functions.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1x capability on ports 1-10:

```
local>config 802.1x capability ports 1 – 10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

 Success.

local>
```

config 802.1x auth_parameter	
Purpose	Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	**config 802.1x auth_parameter ports [<portlist>|all] [default|{direction [both|in]|port_control [force_unauth|auto|force_auth]| quiet_period <sec 0-65535>| max_req <value 1-10>|reauth_period <sec 1-65535>|enable_reauth [enabled|disabled]}]**
Description	The config 802.1x auth_parameter command is used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Parameters	<portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch. default – Returns all of the ports in the specified range to their 802.1x default settings. direction [both|in] – Determines whether a controlled port blocks communication in both the

config 802.1x auth_parameter	
	receiving and transmitting directions, or just the receiving direction. port_control – Configures the administrative control over the authentication process for the range of ports. force_auth – Forces the Authenticator for the port to become authorized. Network access is allowed. auto – Allows the port's status to reflect the outcome of the authentication process. force_unauth – Forces the Authenticator for the port to become unauthorized. Network access will be blocked. quiet_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authenticaiton attempt. max_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user). reauth_period <sec 1-65535> – Configures the time interval between successive re-authentications. enable_reauth [enabled|disabled] – Determines whether or not the switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
local>config 802.1x auth_parameter ports 1 – 20 direction both

Command: config 802.1x auth_parameter ports 1-20 direction
both


 Success.


local>
```

config 802.1x init	
Purpose	Used to initialize the 802.1x functions on a range of ports.
Syntax	**config 802.1x init port_based ports [<portlist>|all]|mac_based ports [<portlist>|all]| {mac_address <macaddr>}**
Description	The config 802.1x init command is used to immediately initialize the 802.1x functions on a range of ports.
Parameters	port_based|mac_based ports – The switch allows you to configure 802.1x by either port or MAC address. <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To initialize 802.1x port-based functions on ports 1 to 15:

```
local>config 802.1x init port-based ports 1-15
Command: config 802.1x init port-based ports 1-15

 Success.

local>
```

config 802.1x reauth	
Purpose	Used to configure the 802.1x re-authentication feature of the switch.
Syntax	**config 802.1x reauth port_based ports [<portlist>|all] | mac_based ports [<portlist>|all] {mac_address <macaddr>}**
Description	The config 802.1x reauth command is used to enable the 802.1x re-authentication feature on the switch.
Parameters	port_based|mac_based ports – The switch allows you to reauthenticate 802.1x by either port or MAC address. <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1x reauthentication for ports 1-15:

```
local>config 802.1x reauth port_based ports 1-15
Command: config 802.1x reauth port_based ports 1-15

 Success.

local>
```

config 802.1x auth_mode	
Purpose	Used to configure the 802.1x authentication mode feature of the switch.
Syntax	**config 802.1x reauth port_based ports [<portlist>|all] | mac_based ports [<portlist>|all] {mac_address <macaddr>}**
Description	The config 802.1x authentication mode command is used to enable either the port-based or MAC-based 802.1x authentication feature on the switch.
Parameters	port_based|mac_based ports – The switch allows you to authenticate 802.1x by either port or MAC address. <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the 802.1x port-based authentication mode for ports 5-6:

```
local>config 802.1x auth_mode port_based ports 5-6
Command: config 802.1x auth_mode port_based ports 5-6

 Success.

local>
```

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

Example Usage:

To configure Radius server communication settings:

```
local>config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

local>
```

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 three 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:

```
local>config radius delete 1

Command: config radius delete 1


 Success.


local>
```

config radius	
Purpose	Used to configure the switch's Radius settings.
Syntax	**config radius <server_index 1-3> {ipaddress <server_ip> {ipaddress <server_ip>|key <passwd 32>|auth_port <udp_port_number>|acct_port <udp_port_number>}**
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 three groups of Radius server settings can be entered on the switch. <server_ip> – The IP address of the Radius server. key – Specifies that a password and encryption key will be used between the switch and the Radius server. <passwd 32> – The shared-secret key used by the Radius server and the switch. Up to 32 characters can be used. default – Returns all of the ports in the range to their default Radius settings. auth_port <udp_port_number> – The UDP port number for authentication requests. The default is 1812. acct_port <udp_port_number> – The UDP port number for accounting requests. The default is 1813.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure Radius settings:

```
local>config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

 Success.

local>
```

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:

```
local>show radius
Command: show radius

Index  IP Address       Auth-Port Number   Acct-Port Number   Status      Key
-----  ---------------   ---------          ---------          ----------  ----------
1      10.1.1.1          1812               1813               Active      switch
2      20.1.1.1          1800               1813               Active      des3250
3      30.1.1.1          1812               1813               Active      dlink

Total Entries : 3

local>
```

22

ACCESS CONTROL LIST (ACL) COMMANDS

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

Command	Parameters
create access_profile	**ethernet** **vlan** **source_mac <macmask>** **destination_mac <macmask>** **802.1p** **ethernet_type** **ip** **vlan** **source_ip_mask <netmask>** **destination_ip_mask <netmask>** **dscp** **icmp** **type**

Command	Parameters
	code igmp type tcp src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> udp udp src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xfff> protocol_id user_mask <hex 0x0-0xffffffff> permit deny profile_id <value 1-255>}
delete access_profile	Profile_id <value 1-255>
config access_profile	profile_id <value 1-255> add access_id <value 1-255> ethernet vlan <vlan_name 32> source_mac <macaddr> destination_mac <macaddr> 802.1p <value 0-7> ethernet_type <hex 0x0-0xfff> ip vlan <vlan_name 32>

Command	Parameters
	source_ip <ipaddr> **destination_ip <ipaddr>** **dscp <value>** **icmp** **type <value 0-255>** **code <value 0-255>** **igmp** **type <value 0-255>** **tcp** **src_port <value 0-65535>** **dst_prot <value 0-65535>** **udp** **src_port <value 0-65535>** **dst_port <value 0-65535>** **protocol_id <value 0-255>** **user_define <hex 0x0-0xffffffff>** **priority <value 0-7>** **replace_priority** **replace_dscp <value 0-63>** **delete <value 1-255>**

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

Access profiles allow you to establish criteria to determine whether the switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a VLAN-by-VLAN basis.

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

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1 deny

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

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

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

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1

Here we use the **profile_id 1** which was specified when the access profile was created. The **add** parameter instructs the switch to add the criteria that follows to the list of rules that are associated with access

profile 1. For each rule entered into the access profile, you can assign an **access_id** that both identifies the rule and establishes a priority within the list of rules. A lower **access_id** gives the rule a higher priority. In case of a conflict in the rules entered for an access profile, the rule with the highest priority (lowest **access_id**) will take precedence.

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

create access_profile	
Purpose	Used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	**create access_profile [ethernet {vlan|source_mac <macmask>|destination_mac <macmask> |802.1p|ethernet_type}|ip {vlan|source_ip_mask <netmask>|destination_ip_mask <netmask>|dscp|[icmp {type|code}|igmp {type}|tcp {src_port_mask <hex 0x0-0xffff>|dst_port_mask <hex 0x0-0xffff>}|udp {src_port_mask <hex 0x0-0xfff>|dst_port_mask <hex 0x0-0xffff>}|protocol_id {user_mask <hex 0x0-0xffffffff>}]}]{[permit|deny]|profile_id <value 1-255>}**
Description	The create access_profile command is used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Parameters	ethernet – Specifies that the switch will examine the layer 2 part of each packet header.

create access_profile

vlan – Specifies that the switch will examine the VLAN part of each packet header.

source_mac <macmask> – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format,

destination_mac <macmask> – Specifies a MAC address mask for the destination MAC address.

802.1p – Specifies that the switch will examine the 802.1p priority value in the frame's header.

ethernet_type – Specifies that the switch will examine the Ethernet type value in each frame's header.

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

vlan – Specifies a VLAN mask.

source_ip_mask <netmask> – Specifies an IP address mask for the source IP address.

destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.

dscp – Specifies that the switch will examine the DiffServ Code Point (DSCP) field in each frame's header.

icmp – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.

type – Specifies that the switch will examine each frame's ICMP Type field.

code – Specifies that the switch will examine each frame's ICMP Code field.

create access_profile

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.

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

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

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

protocol_id – Specifies that the switch will examine each frame's Protocol ID field.

user_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.

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

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

profile_id <value 1-255> – Specifies an index number that will identify the access profile being created with this command.

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

Example Usage:

To create an access profile that will deny service to the subnet ranging from 10.42.73.0 to 10.42.73.255:

```
local> create access_profile ip source_ip_mask 255.255.255.0
profile_id 1 deny

Command: create access_profile ip source_ip_mask
255.255.255.0 profile_id 1 deny


Success.


local>
```

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

Example Usage:

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

```
local> delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

local>
```

config access_profile	
Purpose	Used to configure an access profile on the switch and to define specific values that will be used to by the switch to determine if a given packet should be forwarded or filtered. Masks entered using the create access_profile command will be combined, using a logical AND operation, with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	**config access_profile profile_id <value 1-255> [add access_id <value 1-255>] [ethernet {vlan <vlan_name 32>|source_mac <macaddr>|destination_mac <macaddr>|802.1 <value 0-7>|ethernet_type <hex 0x0-0xffff>|ip{vlan <vlan_name>|source_ip <ipaddr>|destination_ip <ipaddr>|dscp <value 0-63>|[icmp {type <value 0-65535> code <value 0-255>}|igmp {type <value 0-255>}|tcp {src_port <value 0-65535>|dst_port <value 0-65535>}| udp {src_port <value 0-65535>|dst_port <value 0-65535>}|protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]}]{priority <value 0-7> {replace_priority}|replace_dscp <value 0-63>}|delete <value 1-255>]**
Description	The config access_profile command is used to configure an access profile on the switch and to enter specific values that will be combined, using a logical AND operation, with masks entered with the create access_profile command, above.
Parameters	profile_id <value 1-255> –

config access_profile	
	add access_id <value 1-255> – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. A lower access ID, the higher the priority the rule will be given. ethernet – Specifies that the switch will look only into the layer 2 part of each packet. vlan <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN. source_mac <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address. 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 hexidecimal 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 to 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.

config access_profile

dscp <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.

icmp – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field within each packet.

type <value 0-65535> – Specifies that the access profile will apply to this ICMP type value.

code <value 0-255> – Specifies that the access profile will apply to this ICMP code.

igmp – Specifies that the switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

type <value 0-255> – Specifies that the access profile will apply to packets that have this IGMP type value.

tcp – Specifies that the switch will exmamine 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.

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.

config access_profile	
	dst_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header. protocol_id <value 0-255> – Specifies that the switch will examine the Protocol field in each packet and if this field contains the value entered here, apply the following rules. user_define <hex 0x0-0xffffff> – Specifies a mask to be combined with the value found in the frame header using a logical AND operaiton. priority <value 0-7> – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header. replace_priority – This parameter is specified if you want to change the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being transmitted from the switch. replace_dscp <value 0-63> – Allows you to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet. delete <value 1-255> – Specifies that the access ID of a rule you want to delete.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
local>config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1

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


Success.


local>
```

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

Example Usage:

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

```
local>
Access Profile Table

Access Profile  ID:1                              Mode : Deny
                                                  TYPE : IP
==================================================
MASK  Option  Source IP MASK
                  255.255.255.0
-------------------  ----------------------
Access ID
-------------------  ----------------------
1                    10.42.73.0

local>
```

23

ROUTING TABLE COMMANDS

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

Command	Parameters
create iproute	default <ipaddr> <metric 1-65535>
delete iproute	default
show iproute	

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

create iproute	
Purpose	Used to create an IP route entry to the switch's IP routing table.
Syntax	**create iproute default <ipaddr> {<metric 1-65535>}**
Description	This command is used to create an IP route entry to the switch's IP routing table.
Parameters	default – creates a default IP route entry. <ipaddr> – The IP address for the next hop router. <metric 1-65535> – The default setting is 1.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an IP route for the routing table:

```
local>create iproute default 10.1.1.5
Command: create iproute default 10.1.1.5

 Success.

local>
```

delete iproute default	
Purpose	Used to delete an IP route entry from the switch's IP routing table.
Syntax	**delete iproute default**
Description	This command will delete an existing entry from the switch's IP routing table.
Parameters	default – deletes a default IP route entry.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete the default IP route from the switch's routing table:

```
local>delete iproute default
Command: delete iproute default

 Success.

local>
```

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

Example Usage:

To display the contents of the IP routing table:

```
local>show iproute
Command: show iproute

Routing Table
IP Address|Netmask  Gateway     Interface      Hops         Protocol
--------------------------- --------------- --------------- ------------ ------------
10.0.0.0|8                0.0.0.0         System         1            Local

Total Entries  : 1

local>
```

24

SNTP COMMANDS

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

Command	Parameters
config sntp	primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>
enable sntp	
disable sntp	
show sntp	

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

config sntp	
Purpose	Used to configure SNTP on the switch.
Syntax	**config sntp**
Description	This command is used to configure SNTP on the switch.
Parameters	primary – This is the primary server the SNTP information will be taken from. <ipaddr> – The IP address of the primary server. secondary – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable. <ipaddr> – The IP address for the secondary server. poll-interval – This is the time the SNTP information will be polled. <int 30-99999> – The polling interval ranges from 30 to 99,999 seconds.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure SNTP for the primary server for a switch.

```
local>config sntp primary 10.24.22.5
Command: config sntp primary 10.24.22.5

 Success.

local>
```

enable sntp	
Purpose	Used to enable SNTP on the switch.
Syntax	**enable sntp**
Description	This command enables SNTP on a switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable SNTP on the switch:

```
local>enable sntp
Command: enable sntp

 Success.

local>
```

disable sntp	
Purpose	Used to disable SNTP on the switch.
Syntax	**disable sntp**
Description	This command will disable SNTP on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To disable SNTP on the switch:

```
local>disable sntp
Command: disable sntp

Success.

local>
```

show sntp	
Purpose	Used to show SNTP on the switch.
Syntax	**show sntp**
Description	This command will show SNTP on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show SNTP on the switch:

```
local>show sntp
Command: show sntp

   Current Time Source      : System Clock
   SNTP  :  Disabled
   SNTP Primary Server      : 10.24.22.5
   SNTP Secondary Server  : 0.0.0.0
   SNTP poll interval  :  720 sec

local>
```

26

COMMAND HISTORY LIST

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

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

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

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

Example Usage:

To display all of the commands in the CLI:

```
local>?
Command: ?
..
?
clear
clear counters
clear fdb
clear log
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
```

```
config account
config bandwidth_control
config command_history
config command_prompt
config fdb aging_time
config gvrp
config igmp_snooping
config igmp_snooping querier
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

show command_history	
Purpose	Used to display the command history.
Syntax	**show command_history**
Description	This command will display the command history.
Parameters	none.
Restrictions	none.

Example Usage:

To display the command history:

```
local>show command_history
Command: show command_history

clear
show
command history
clear
close
show command history
show ?
show
show command history
?

local>
```

dir	
Purpose	Used to display all commands.
Syntax	**dir**
Description	This command will display all commands.
Parameters	none.
Restrictions	none.

Example Usage:

To display all of the commands:

```
local>dir
Command: dir
..
?
clear
clear counters
clear fdb
clear log
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config bandwidth _control
```

```
config command_history
config command_prompt
config fdb aging_time
config gvrp
config igmp_snooping
config igmp_snooping querier
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

config command_history	
Purpose	Used to configure the command history.
Syntax	**config command_history <value 1-40>**
Description	This command is used to configure the command history.
Parameters	<value 1-40> –
Restrictions	none.

Example Usage:

To configure the command history:

```
local>config command_history 20
Command: config command_history 20

 Success.

local>
```

A

TECHNICAL SPECIFICATIONS

	General	
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX Gigabit Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3 Nway auto-negotiation	
Protocols:	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	n|a	2000Mbps
Topology:	Star	

General	
Network Cables: 10BASE-T:	 2-pair UTP Cat. 3,4,5 (100 m) EIA/TIA- 568 100-ohm STP (100 m)
100BASE-TX:	2-pair UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)
Mini GBIC:	IEC 793-2:1992 Type A1a - 50|125um multimode Type A1b - 62.5|125um multimode (SC optical connector)
Number of Ports:	48x 10/100 Mbps NWay ports 2 Gigabit Ethernet ports – 1000BASE-T (included) or Mini GBIC (optional)

Physical and Environmental	
AC input & External Redundant power Supply:	100 – 120; 200 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	30 watts maximum
DC fans:	2 built-in 40 x 40 x10 mm fans
Operating Temperature:	0 to 40 degrees Celsius
Storage Temperature:	-40 to 70 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing

Physical and Environmental	
Dimensions:	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width
Weight:	4.4 kg
EMI:	FCC Class A, CE Class A, BSMI Class A, C-Tick Class A
Safety:	CSA International

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	64M Bytes per device
Filtering Address Table:	8K MAC address per device
Packet Filtering| Forwarding Rate:	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps) 1,488,000 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age:10–9999 seconds. Default = 300.

B

SWITCH SYSTEM MESSAGES

NO.	Message	Remark
1	"Success."	
2	"Error applying data!"	
3	"Invalid IP address!"	
4	"Invalid subnet mask!"	
5	"Invalid gateway address!"	
7	"All changes are saved!"	
8	"Invalid MAC address!"	
9	"No more MAC-Based VLANs can be added!"	
10	"No more MAC addresses can be added!"	

11	"Invalid VLAN Description!"	
12	"The entry does not exist."	
13	"Duplicate IP address! Enter a unique IP address."	
14	"Invalid metrics!"	
15	"Flow Control is not Enabled!"	
16	"Spanning tree group name cannot be empty!"	
17	"The IP interface must be deleted first!"	
18	"The system interface is not in manual mode!"	
19	"The VLAN already has a IP Interface!"	
20	"The specified IGMP snooping entry cannot be modified."	
21	"You have more than 255 IGMP snooping entries."	
22	"IGMP state in the VLAN is disabled or current VID is invalid!"	
23	"The external module port is not exist."	
24	"You must select at least one port member!"	
25	"Target mirror port can't be set in the trunk, please change it first!"	
26	"Invalid port or width setting!"	

27	"Untagged ports overlapped!"	
28	"Invalid VLAN name!"	
29	"Invalid duplicate VLAN ID!"	
30	"Incorrect aging time specified. The value must be from 300 to 1000000!"	
31	"The specified entry is not found!"	
32	"All changes applied BUT trunk member follows master!"	
33	"Master port can't be half-duplex mode!"	
34	"The EEPROM is full!"	
35	"The VLAN has no router ports."	
36	"IGMP snooping is disabled in the designated VLAN."	
37	"The username is invalid."	
38	"Incorrect password"	
39	"The specified user already exists. Enter a unique username."	***Add user***
40	"The username does not exist. Enter the name of an existing user"	***Delete and Update user.***
41`	"One active Admin user must exist!"	***Delete or Update user.***
42	"Confirmation error! Passwords do not match."	***Add or Update user.***
43	"No more user accounts can be added!"	***Add user.***

44	"Please wait, loading factory parameters....."	
45	"You need to configure a port within the range selected to view!"	
46	"Invalid port settings!"	
47	"The TFTP process was stopped!"	
48	"Cannot upload log. The switch does not have a history log!"	
49	"The maximum number of spanning tree group is twelve!"	
50	"MAC address must be unicast!"	
51	"MAC address must be multicast!"	
52	"Forwarding|Filtering Table is full!"	
53	"Multicast member must exist in the VLAN."	
54	"The member port must exist in the VLAN."	
55	"Duplicate route! Enter a unique route."	
56	"Target port can't be source port!"	
57	"This port member can't be set."	
58	"Port members must belong to the same VLAN."	
59	"The target port can't be selected as a mirror port."	

60	"Invalid or undefined VID!"	
61	"Specified vid is not in the static VLAN table."	
62	"This is the DEFAULT_VLAN, it cannot be removed."	
63	"This VLAN is used by routing interface, it cannot be removed."	
64	"Invalid VLAN name."	
65	"The VLAN name you entered is existing."	
66	"The VLAN name you entered does not exist."	Check IP Address or VLAN name.
67	"Invalid Interface name."	Check Interface Name.
68	"The interface name already exists. Enter a unique interface name."	Check Interface Name.
69	"The interface name does not exist."	Check Interface Name.
70	"VLAN table is full!"	
71	"The specified VID has no MAC addresses."	
72	"The specified port has no MAC addresses."	
73	"Port Based VLAN overlapped!"	
74	"Default VLAN can't be deleted."	
75	"VLAN name overlapped!"	

76	"You can't delete the VLAN which is used by IP subnet!"	
77	"The system IP interface can't be deleted."	
78	"Invalid IP address or invalid number of pings."	
79	"Search entry is not found!"	
80	"Membership can't be overlap!"	
81	"The default entry can't be deleted!"	
82	"Non-egress port must set to TAG!"	

Variable Name	***Maxmum Length***	***Type***
<username>	15	String
<password>	15	String
<ipaddr>	15	IP-Address
<netmask>	15	IP-Address
<gateway>	15	IP-Address
<vlan_name>	32	String
<sw_name>	128	String
<sw_location>	128	String

<sw_contact>	128	String
Password	15	String
<community_string>	32	String
<server_ip>	15	IP-Address
<path_filename>	64	String
<macaddr>	17	MAC-Address
<ipif>	12	String

D-Link® Offices

Australia

D-Link Australasia
1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia
TEL: 61-2-8899-1800 FAX: 61-2-8899-1868
TOLL FREE (Australia): 1300 766 868
TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au
E-MAIL: support@dlink.com.au & info@dlink.com.au

Brazil

D-Link Brasil Ltda.
Rua Tavares Cabral 102 - Conj. 31 e 33
05423-030 Pinheiros, Sao Paulo, Brasil
TEL: (5511) 3094 2910 to 2920 FAX: (5511) 3094 2921
URL: www.dlink.com.br

Canada

D-Link Canada
2180 Winston Park Drive, Oakville,
Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223
BBS: 1-965-279-8732 FTP: ftp.dlinknet.com
TOLL FREE: 1-800-354-6522
URL: www.dlink.ca E-MAIL: techsup@dlink.ca

Chile

D-Link South America (Sudamérica)
Isidora Goyenechea 2934
Oficina 702, Las Condes, Santiago, Chile
TEL: 56-2-232-3185 FAX: 56-2-232-0923
URL: www.dlink.com.cl

China

D-Link Beijing
Level 5,Tower W1,The Tower,Oriental Plaza
No.1,East Chang An Ave., Dong Cheng District
Beijing,100738,China
TEL: (8610) 85182529/30/31/32/33
FAX: (8610) 85182250
URL: www.dlink.com.cn E-MAIL:
webmaster@dlink.com.cn

Denmark

D-Link Denmark
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL: 45-43-969040 FAX: 45-43-424347
URL: www.dlink.dk E-MAIL: info@dlink.dk

Egypt

D-Link Middle East
7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt
TEL: 202-624-4615 FAX: 202-624-583
URL: www.dlink-me.com
E-MAIL: support@dlink-me.com & dlinkegypt@dlink-me.com

Finland

D-Link Finland
Pakkalankuja 7A, 01510 Vantaa, Finland
TEL: 358-9-2707-5080 FAX: 358-9-2707-5081
URL: www.dlink-fi.com

France

D-Link France
Le Florilege, No. 2, Allée de la Fresnerie,
78330 Fontenay-le-Fleury, France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689
URL: www.dlink-france.fr
E-MAIL: info@dlink-france.fr

Germany

D-Link Central Europe (D-Link Deutschland GmbH)
Schwalbacher Strasse 74, D-65760 Eschborn, Germany
TEL: 49-6196-77990 FAX: 49-6196-7799300
BBS: 49-(0) 6192-971199 (analog) & BBS: 49-(0) 6192-971198 (ISDN)
INFO: 00800-7250-0000 (toll free) & HELP: 00800-7250-4000 (toll free)
REPAIR: 00800-7250-8000 & HELP: support.dlink.de
URL: www.dlink.de & E-MAIL: info@dlink.de

India

D-Link India
Plot No.5, Kurla -Bandra Complex Rd., Off Cst Rd.,
Santacruz (East), Mumbai, 400 098 India
TEL: 91-022-2652-6696/6788/6623
FAX: 91-022-2652-8914/8476
URL: www.dlink.co.in
E-MAIL: service@dlink.co.in & tushars@dlink.co.in

Italy

D-Link Mediterraneo Srl/D-Link Italia
Via Nino Bonnet n. 6/B, 20154, Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723
URL: www.dlink.it E-MAIL: info@dlink.it

Japan	**D-Link Japan** 10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp E-MAIL: kida@d-link.co.jp
Netherlands	**D-Link Benelux** Lichtenauerlaan 102-120, 3062 ME Rotterdam, Netherlands TEL: +31-10-2045740 FAX: +31-10-2045880 URL: www.d-link-benelux.nl & www.dlink- benelux.be E-MAIL: info@dlink-benelux.com
Norway	**D-Link Norway** Karihaugveien 89, 1086 Oslo TEL: 47-22-309075 FAX: 47-22-309085 SUPPORT: 800-10-610 & 800-10-240 (DI-xxx) URL: www.dlink.no
Russia	**D-Link Russia** 129626 Russia, Moscow, Graphskiy per., 14, floor 6 TEL/FAX: +7 (095) 744-00-99 URL: www.dlink.ru E-MAIL: vl@dlink.ru
Singapore	**D-Link International** 1 International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-6774-6233 FAX: 65-6774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com
South Africa	**D-Link South Africa** Einstein Park II, Block B 102-106 Witch-Hazel Avenue Highveld Technopark Centurion, Gauteng, Republic of South Africa TEL: +27-12-665-2165 FAX: +27-12-665-2186 URL: www.d-link.co.za E-MAIL: attie@d-link.co.za
Spain	**D-Link Iberia S.L.** Sabino de Arana, 56 bajos, 08028 Barcelona, Spain TEL: 34 93 409 0770 FAX: 34 93 491 0795 URL: www.dlink.es E-MAIL: info@dlink.es

Sweden

D-Link Sweden
P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-8-564-61900 FAX: 46-8-564-61901
URL: www.dlink.se E-MAIL: info@dlink.se

Taiwan

D-Link Taiwan
2F, No. 119, Pao-chung Road, Hsin-tien, Taipei, Taiwan
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw E-MAIL: dssqa@dlinktw.com.tw

Turkey

D-Link Turkiye
Beybi Giz Plaza, Ayazaga Mah. Meydan Sok. No. 28
Maslak 34396, Istanbul-Turkiye
TEL: 90-212-335-2553 (direct) & 90-212-335-2525 (pbx)
FAX: 90-212-335-2500 E-MAIL: dlinkturkey@dlink-me.com
E-MAIL: support@dlink-me.com

U.A.E.

D-Link Middle East FZCO
P.O. Box18224 R/8, Warehouse UB-5
Jebel Ali Free Zone, Dubai – United Arab Emirates
TEL: (Jebel Ali): 971-4-883-4234
FAX: (Jebel Ali): 971-4-883-4394 & (Dubai): 971-4-335-2464
E-MAIL: dlinkme@dlink-me.com & support@dlink-me.com

U.K.

D-Link Europe (United Kingdom) Ltd
4th Floor, Merit House, Edgware Road, Colindale, London
NW9 5AB United Kingdom
TEL: 44-020-8731-5555 SALES: 44-020-8731-5550
FAX: 44-020-8731-5511 SALES: 44-020-8731-5551
BBS: 44 (0) 181-235-5511
URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A.

D-Link U.S.A.
53 Discovery Drive, Irvine, CA 92618, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033
INFO: 1-800-326-1688 URL: www.dlink.com
E-MAIL: tech@dlink.com & support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr.|Ms_____

Organization: _____ Dept. _____

Your title at organization: _____

Telephone: _____ Fax:_____

Organization's full address: _____

_____

Country: _____

Date of purchase (Month|Day|Year): _____

Product Model	**Product Serial No.**	*** Product installed in type of computer (e.g., Compaq 486)**	*** Product installed in computer serial No.**

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____

Telephone: _____ Fax:_____

Reseller's full address: _____

_____

_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?

☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?

☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?

☐XNS|IPX ☐TCP|IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?

☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix|Xenix ☐PC NFS ☐3Com 3+Open

☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95

☐Others_____

5. What network management program does your organization use ?

☐D-View ☐HP OpenView|Windows ☐HP OpenView|Unix ☐SunNet Manager ☐Novell NMS

☐NetView 6000 ☐Others_____

6. What network medium|media does your organization use ?

☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP|STP

☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?

☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD|CAM

☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?

☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance|Real Estate ☐Manufacturing

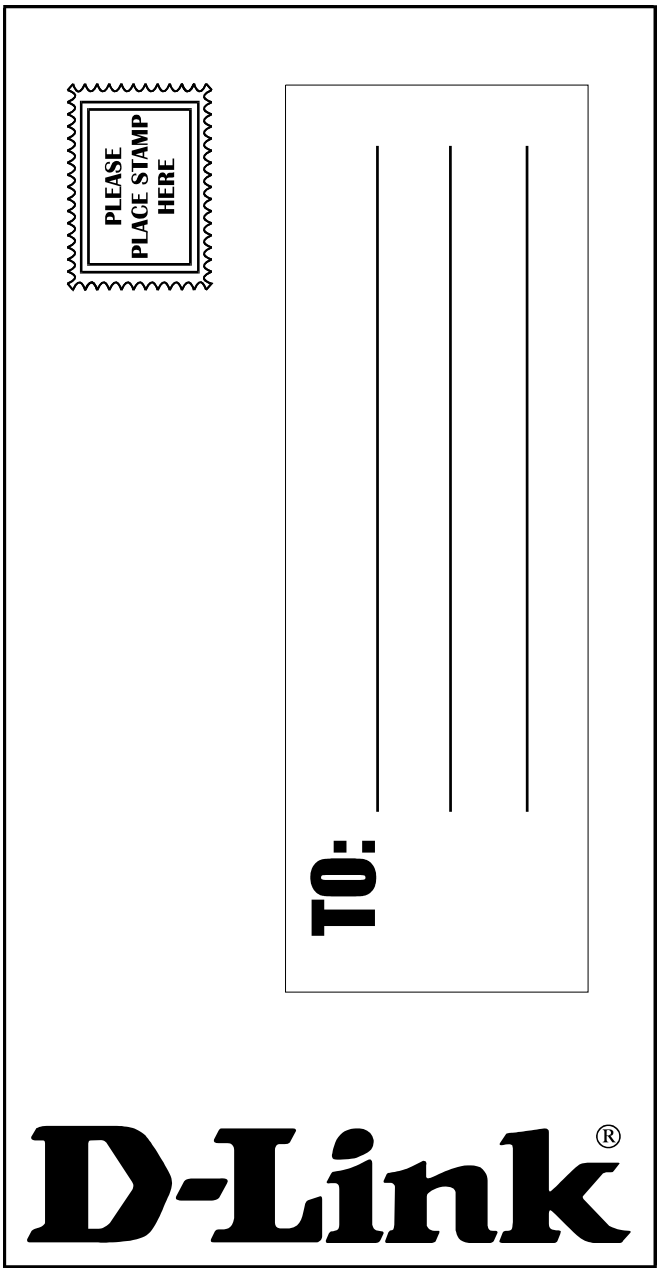
☐Retail|Chainstore|Wholesale ☐Government ☐Transportation|Utilities|Communication ☐VAR

☐System house|company ☐Other_____

9. Would you recommend your D-Link product to a friend?

☐Yes ☐No ☐Don't know yet

10.Your comments on this product?


PLEASE
PLACE STAMP
HERE
TO:
D-Link®