D-Link®

DES-3250G

Layer 2 Switch

Command Line Interface
Reference Manual

First Edition (February 2003)
DES3250TG.A1
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.

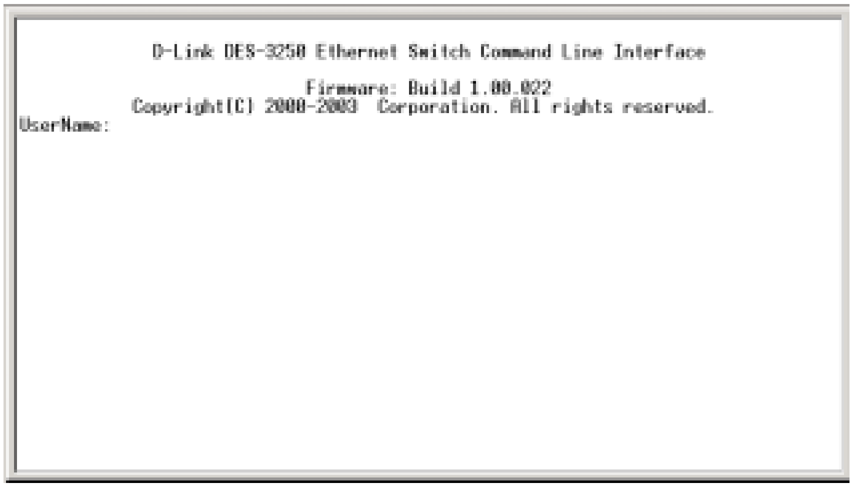
Accessing the Switch via the Serial Port

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/ANSI 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.



```
              D-Link DES-3250 Ethernet Switch Command Line Interface

                            Firmware: Build 1.00.022
           Copyright(C) 2000-2003  Corporation. All rights reserved.
UserName:
```

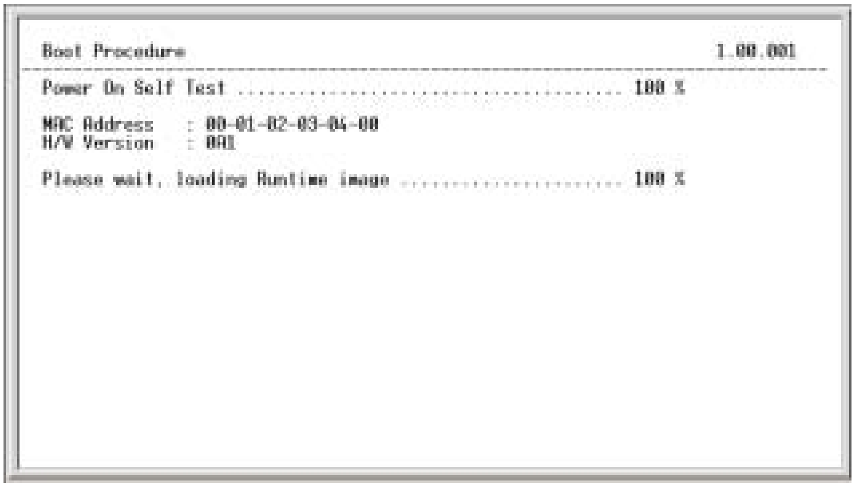
Figure 1-1. Initial Console screen.

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.



```
Boot Procedure                                                    1.00.001
------------------------------------------------------------------------------
Power On Self Test ....................................... 100 %

MAC Address    : 00-01-02-03-04-00
H/W Version    : 0A1

Please wait, loading Runtime image ....................... 100 %
```

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.

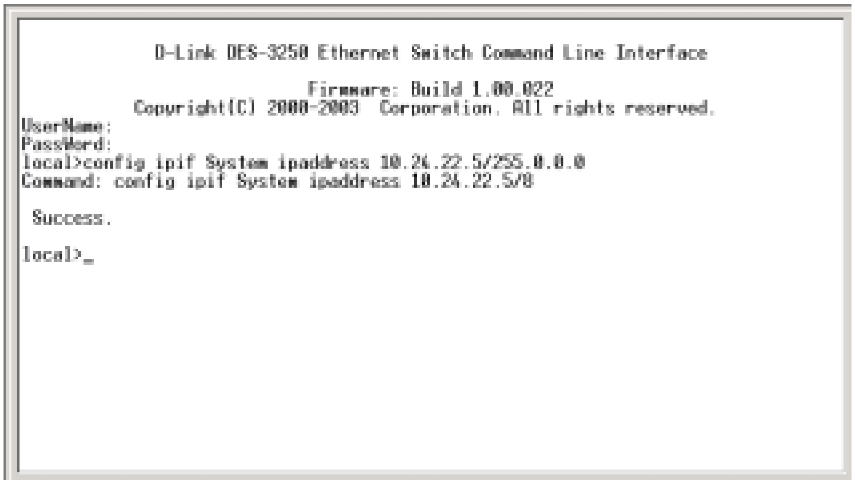
The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

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.



```
            D-Link DES-3250 Ethernet Switch Command Line Interface

                          Firmware: Build 1.00.022
          Copyright(C) 2000-2003  Corporation. All rights reserved.
UserName:
PassWord:
local>config ipif System ipaddress 10.24.22.5/255.0.0.0
Command: config ipif System ipaddress 10.24.22.5/8

 Success.

local>_
```

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 an SNMP-based network management software over the network.

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

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.

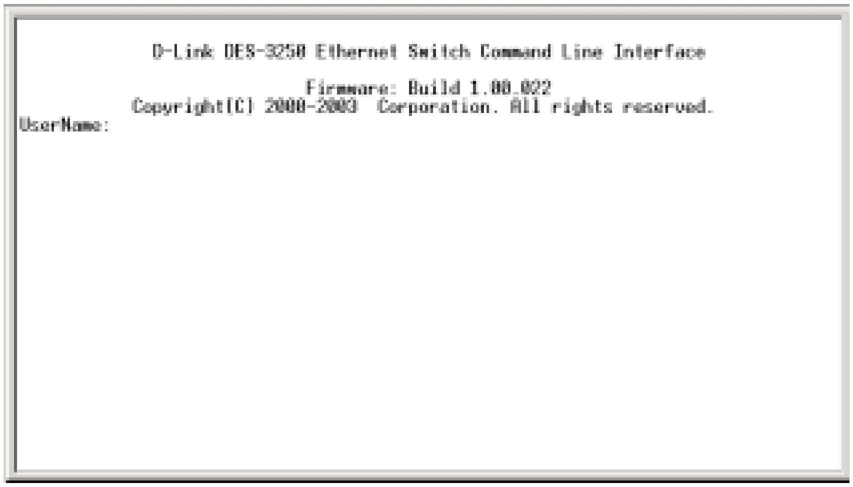
Connecting to the Switch

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/ANSI 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:



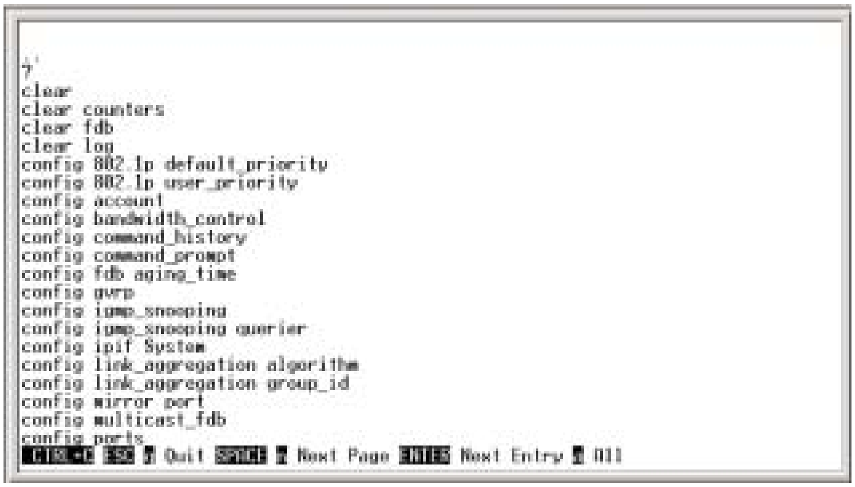
```
            D-Link DES-3250 Ethernet Switch Command Line Interface

                          Firmware: Build 1.00.022
          Copyright(C) 2000-2003  Corporation. All rights reserved.
UserName:
```

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.



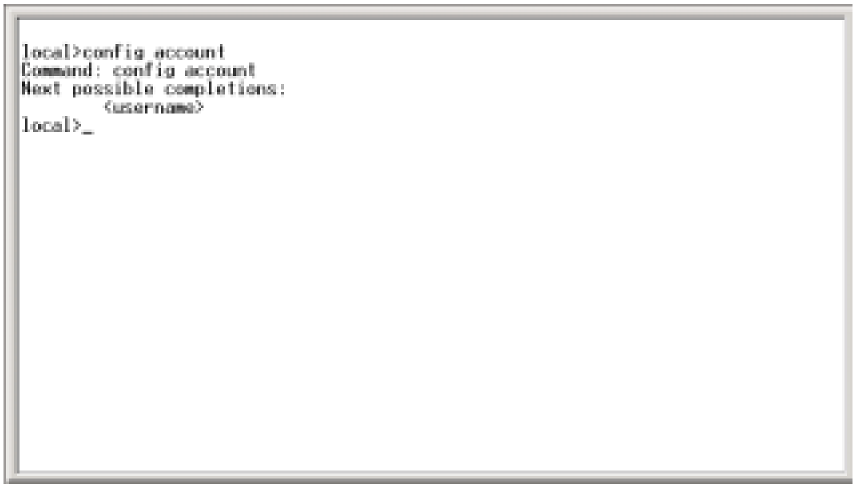
```
?
clear
clear counters
clear fdb
clear log
config 802.1p default_priority
config 802.1p user_priority
config account
config bandwidth_control
config command_history
config command_prompt
config fdb aging_time
config gvrp
config igmp_snooping
config igmp_snooping querier
config ipif System
config link_aggregation algorithm
config link_aggregation group_id
config mirror port
config multicast_fdb
config ports
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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.

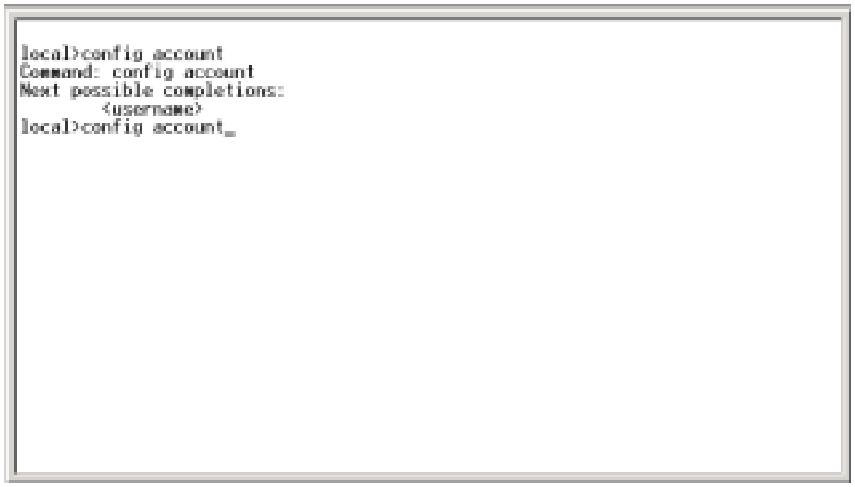


```
local>config account
Command: config account
Next possible completions:
        <username>
local>_
```

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.



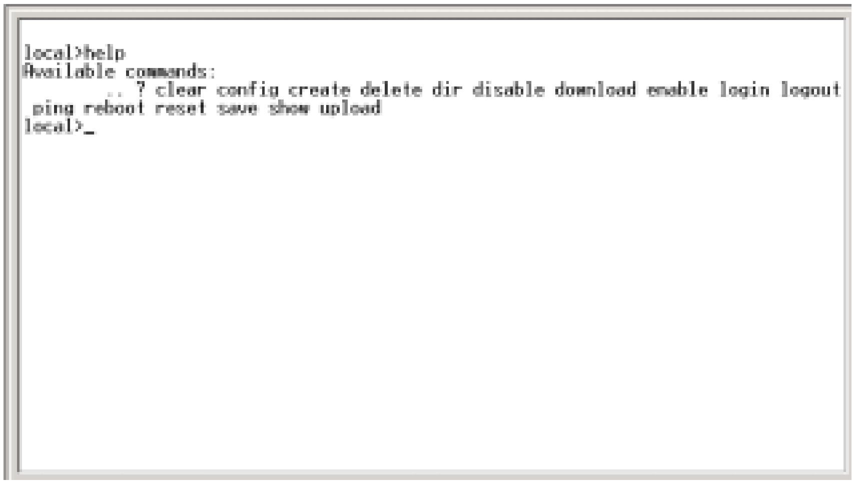
```
local>config account
Command: config account
Next possible completions:
        <username>
local>config account_
```

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.

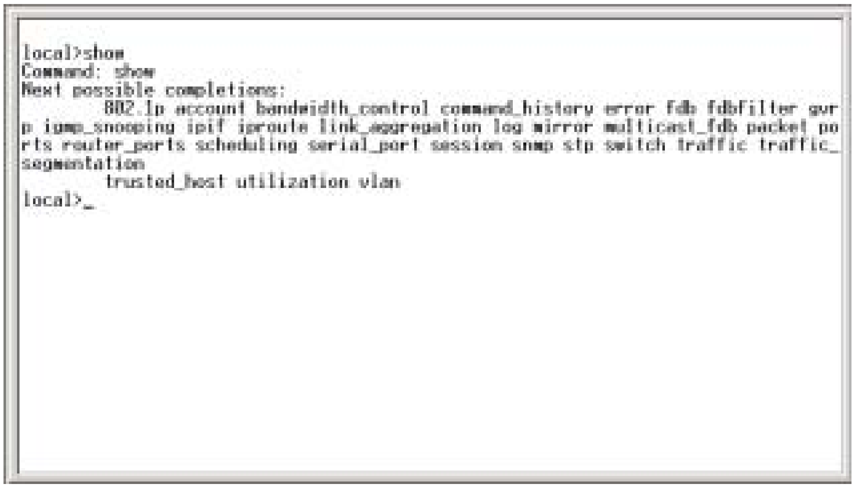


```
local>help
Available commands:
        .. ? clear config create delete dir disable download enable login logout
 ping reboot reset save show upload
local>_
```

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.



```
local>show
Command: show
Next possible completions:
        802.1p account bandwidth_control command_history error fdb fdbFilter gvr
p igmp_snooping ipif iproute link_aggregation log mirror multicast_fdb packet po
rts router_ports scheduling serial_port session snmp stp switch traffic traffic_
segmentation
        trusted_host utilization vlan
local>_
```

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	**create ipif <ipif_name> vlan <vlan_name> ipaddress <network_address>**
Description	In the above syntax example, you must supply an IP interface name in the <ipif_name> space, a VLAN name in the <vlan_name> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	**create ipif Engineering vlan Design 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.
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**

/slash	
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 backslash.
Example Command	**show snmp community**

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	**config igmp [<ipif_name>/all] {version <value>/query_interval <sec>/max_response_time <sec>/ robustness_variable <value>/last_member_query_interval <value>/state [enabled/disabled]}**
Description	In the above syntax example, you must choose to enter an IP interface name in the <ipif_name> space or all, but version <value>, query_interval <sec>, max_response_time <sec>, robustness_variable <value>, last_member_query_interval <value>, and state [enabled/disabled] are all optional arguments. You can specify any or all of the arguments contained by braces. Do not type the braces.
Example command	**config igmp all version 2**

Line Editing Key Usage	
Delete	Deletes character under the cursor and then shifts the remaining characters in the line to the left.

Line Editing Key Usage	
Backspace	Deletes the character to the left of the cursor and shifts the remaining characters in the line to the left.
Insert	Can be toggled on or off. When toggled on, inserts text at the current cursor position and shifts the remainder of the line to the left.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Tab	Shifts the cursor to the next field to the left.
Multiple Page Display Control Keys	
Space	Displays the next page.
CTRL+c	Stops the display of remaining pages when multiple pages are to be displayed.
ESC	Stops the display of remaining pages when multiple pages are to be displayed.
n	Displays the next page.
p	Displays the previous page.
q	Stops the display of remaining pages when multiple pages are to be displayed.
r	Refreshes the pages currently displaying.

Line Editing Key Usage	
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	
enable telnet	<tcp_port_number>
disable telnet	
enable web	<tcp_port_number>

Command	Parameters
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

create account

	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.

config account

	Usernames can be between 1 and 15 characters. Passwords can be between 0 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 8 user accounts can exist on the switch at one time.
Parameters	none.

show account

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
```

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 1.00.001
Firmware Version       : Build 1.00.024
Hardware Version       : 0A1
System Name            :
System Location        :
System Contact         :
Spanning Tree          : Disabled
GVRP                   : Disabled
```

```
IGMP Snooping     : Disabled
TELNET           : Enabled  (TCP 23)
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

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

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.

save

	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.

reset

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.

config ports	
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

config ports

	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

show ports

	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

NETWORK MANAGEMENT COMMANDS

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

Command	Parameters
create snmp community	<community_string> [readonly/readwrite]
delete snmp community	<community_string>
create snmp trap_receiver	<ipaddr> <community_string>
delete snmp trap_receiver	<ipaddr>
enable rmon	
disable rmon	
config snmp community	<community_string> [readonly/readwrite]
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>

Command	Parameters
config snmp system_name	<sw_name>
config snmp trap_receiver	<ipaddr> <community_string>
enable snmp traps	
disable snmp traps	
enable snmp authenticate traps	
disable snmp authenticate traps	
create trusted_host	<ipaddr>
show trusted_host	<ipaddr>
delete trusted_host	<ipaddr>
show snmp	[community/trap_receiver]
ping	<ipaddr> times <value> timeout <sec>

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

create snmp community	
Purpose	Used to create an SNMP community string.
Syntax	**create snmp community <community_string> [readonly/readwrite]**

create snmp community

Description	This command is used to create an SNMP community string and to specify the string as enabling read only or read-write privileges for the SNMP management host.
Parameters	<community_string> – An alphanumeric string of up to 32 characters used to authentication of users wanting access to the switch's SNMP agent. readonly – Allows the user using the above community string to have read only access to the switch's SNMP agent. The default read only community string is public. readwrite – Allows the user using the above community string to have read and write acces to the switch's SNMP agent. The default read write community string is private.
Restrictions	Only administrator-level users can issue this command. A maximum of 4 community strings can be specified.

Example Usage:

To create a read-only level SNMP community "System":

```
local>create snmp community System readwrite
Command: create snmp community System readwrite

 Success.
```

```
local>
```

delete snmp community

Purpose	Used to delete an SNMP community string previously entered on the switch.
Syntax	**delete snmp community <community_string>**
Description	This command is used to delete an SNMP community string entered on the switch using the create SNMP community command above.
Parameters	<community_string> – An alphanumeric string of up to 32 characters used to authentication of users wanting access to the switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a read-only level SNMP community "System":

```
local>delete snmp community System
Command: delete snmp community System

Success.

local>
```

create snmp trap_receiver	
Purpose	Used to specify a management station, by IP address and community string, that will receive traps generated by the switch's SNMP agent.
Syntax	**create snmp trap_receiver <ipaddr> <community_string>**
Description	This command is used to specify the IP address of a management station that will receive traps generated by the switch's SNMP agent and the community string that will be used to authenticate the management station's privileges.
Parameters	<ipaddr> – The IP address of a management station that will receive SNMP traps generated by the switch's SNMP agent.
	<community_string> – An alpha-numeric string of up to 32 characters that will be used to authenticate management stations that want to receive SNMP traps from the switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command. A maximum of 3 trap receivers can be specified.

Example Usage:

To create a trap receiver 10.1.1.1 in read-only level SNMP community:

```
local>create snmp trap_receiver 10.1.1.1 System
Command: create snmp trap_receiver 10.1.1.1 System

Success.

local>
```

delete snmp trap_receiver

Purpose	Used to delete a trap receiver entry on the switch made using create SNMP trap_reciever above.
Syntax	**delete snmp trap_reciever <ipaddr>**
Description	The command allows the user to delete an SNMP trap receiver specified previously using the create trap_receiver command above.
Parameters	<ipaddr> – The IP address of the management station that is currently specified to receive traps from the switch’s SNMP agent. This management station will be deleted from the list of up to three that can be entered using the create SNMP trap_receiver commmand above.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a trap receiver 10.1.1.1:

```
local>delete snmp trap_receiver 10.1.1.1
Command: delete snmp trap_receiver 10.1.1.1

Success.

local>
```

config snmp community

Purpose	Used to create an SNMP community string.
Syntax	**config snmp community <community_string> [readonly/readwrite]**
Description	This command is used to create an SNMP community string on the switch that will be used to authenticate management stations that want to access the switch using SNMP management software.
Parameters	<community_string> – An alpha-numeric string of up to 32 characters that will be used to authenticate management stations that want to access the switch's SNMP agent. readonly – Allows the user using the above community string to have read only access to the switch's SNMP agent. The default read only community string is public. readwrite – Allows the user using the above community string to have read and write access to the switch's SNMP agent. The

config snmp community

	default read write community string is private.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure an SNMP community "System":

```
local>config snmp community System readwrite
Command: config snmp community System readwrite

Success.

Local>
```

config snmp trap_receiver

Purpose	Used to configure an SNMP trap receiver.
Syntax	**config snmp trap_receiver <ipaddr> <community_string>**
Description	This command is used to configure an SNMP trap receiver on the switch that will be used to authenticate management stations that want to access the switch using SNMP management software.
Parameters	<ipaddr> – The IP address of the management station that is currently specified to receive traps from the switch's SNMP agent. This management station will

config snmp trap_receiver

	be deleted from the list of up to three that can be entered using the create SNMP trap_receiver commmand above. <community_string> – An alpha-numeric string of up to 32 characters that will be used to authenticate management stations that want to access the switch’s SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure an SNMP trap receiver “mink” with an IP address of 10.1.1.2:

```
Local>config snmp trap_receiver 10.1.1.2 mink
Command: config snmp trap_receiver 10.1.1.2 mink

Success.

local>
```

config snmp system_name

Purpose	Used to configure a name for the switch.
Syntax	**config snmp system_name <sw_name>**

config snmp system_name

Description	This command is used to give the switch an alpha-numeric name of up to 128 characters.
Parameters	<sw_name> – An alpha-numeric name for the switch of up to 128 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 128 characters can be used.

config snmp system_location

Parameters	<sw_location> – A description of the location of the switch. A maximum of 128 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 128 characters can be used.

config snmp system_contact

Parameters	<sw_contact> – A maximum of 128 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.

enable rmon

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>
```

show snmp

Purpose	Used to display the SNMP configuration entered on the switch.
Syntax	**show snmp [community_string/trap_receiver]**
Description	This command will display the current SNMP configuration on the switch.
Parameters	community_string – Displays all of the community strings configured on the switch. A community string is an alpha-numeric string of up to 32 characters used to authenticate management stations wanting access to the switch's SNMP agent. trap_receiver – Displays all of the trap_receiver IP addresses configured on the switch. A trap receiver is a host on the same subnet as the switch that can receive SNMP trap messages.
Restrictions	none.

Example Usage:

To display SNMP configurations:

```
local>show snmp
Command: show snmp

System Name        : DES3250
System Location    : Taiwan
System Contact      : dlink
SNMP Trap           : Enabled
Authenticate Traps : Enabled


Community String                              Rights
-------------------------------------------             ---------------
System                                          Read/Write
public                                          Read-Only
Develop                                          Read-Only
private                                         Read/Write

 Total Entries: 4

IP Address     Community String
---------------     -----------------------------------------------------------
10.1.1.1        Develop

 Total Entries: 1

local>
```

create trusted_host

Purpose	Used to create trusted hosts.

create trusted_host

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.

show trusted_host

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

delete trusted_host

	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.

enable snmp traps

	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 t 'aps

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>}**

ping	
	<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 4 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>
```

7

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-

download	
	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.

upload	
	<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>
```

8

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>**

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.

show packet ports

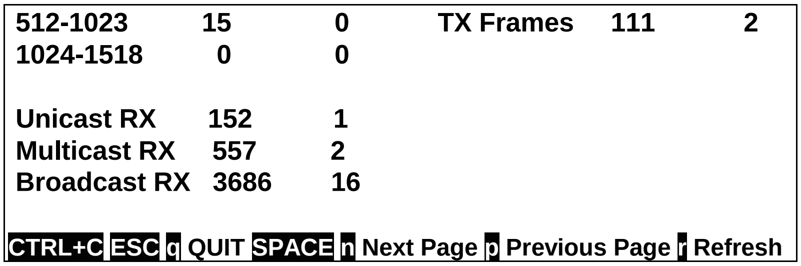
	sent and received by the switch.
Syntax	**show packet ports <portlist>**
Description	This command is used to display statistics about packets sent and received by ports specified in the port list.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing 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 port 7:

```
local>show packet ports 7

Port number : 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

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

show error ports

Purpose	Used to display the error statistics for a range of ports.
Syntax	**show error ports <portlist>**
Description	This command will display all of the packet error statistics collected and logged by the switch for a given port list.
Parameters	<portlist> – Specifies a 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 port 3:

```
Command: show error ports 3

 Port number  :  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

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

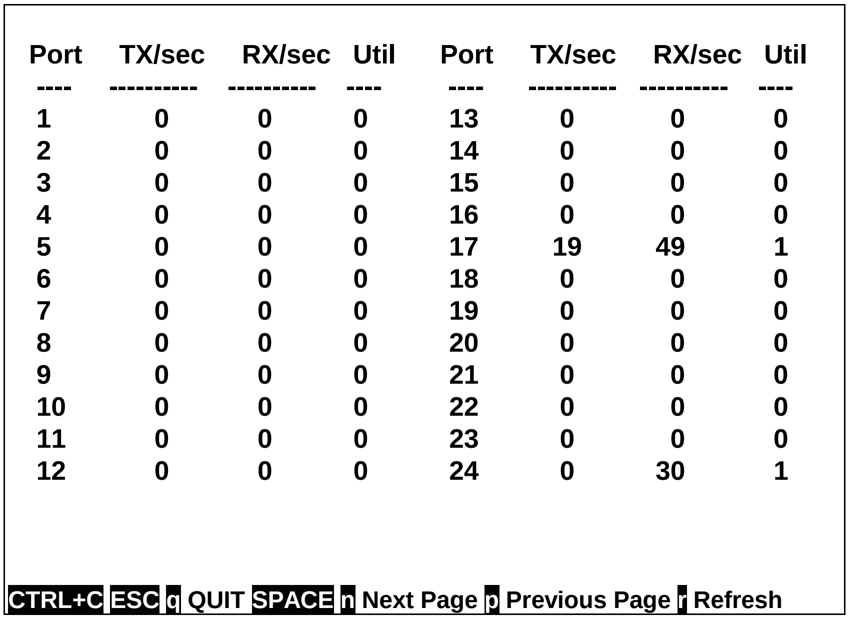
show utilization

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         0         0       0     13       0         0        0
 2         0         0       0     14       0         0        0
 3         0         0       0     15       0         0        0
 4         0         0       0     16       0         0        0
 5         0         0       0     17      19        49        1
 6         0         0       0     18       0         0        0
 7         0         0       0     19       0         0        0
 8         0         0       0     20       0         0        0
 9         0         0       0     21       0         0        0
 10        0         0       0     22       0         0        0
 11        0         0       0     23       0         0        0
 12        0         0       0     24       0        30        1



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

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

clear counters

	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 7-9
Command: clear counters ports 7-9

 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     Successful login through Console (Username:
Anonymous)
3    000d00h50m     Logout through Console (Username:
```

```
Anonymous)
2    000d00h49m     Successful login through Console (Username:
Anonymous)
1      000d00h49m   Logout through Console (Username:
       Anonymous)
local>
```

9

SPANNING TREE COMMANDS

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

Command	Parameters
config stp	**ports <portlist>** **cost <value 1-65535>** **priority <value 0-255>** **state [enabled/disabled]** **maxage <value 6-40>** **hellotime <value 1-10>** **forwarddelay <value 4-30>** **priority <value 0-65535>** **fbpdu [enabled/disabled]**
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 set up STP on the switch.

Syntax

config stp {ports <portlist> {cost <value 1-65535>/priority <value 0-255>/state [enabled/disabled]} {maxage <value 6-40>/hellotime <value 1-10>/forwarddelay <value 4-30>/priority <value 0-65535>/fbpdu [enabled/disabled]}

Description

This command is used to set up the Spanning Tree Protocol (STP) for the entire switch.

Parameters

ports <portlist> – Specifies a range of ports to be configured. Ports are specified by entering the lowest port number in a group, and then the highest port number in a group, separated by a dash. So, a port group including the switch ports 1, 2, and 3 would be entered as 1-3. Ports that are not contained within a group are specified by entering their port number, separated by a comma. So, the port group 1-3 and port 49 would be entered as 1-3, 49. Additional ports can be individually entered by their port number, separated by commas. If you enter the ports sub-command, you can enter the port STP cost, priority, and state sub-commands listed below.

cost <value 1-65535> – This defines a metric that indicates the relative cost of forwarding packets to the specified port

config stp	
	list. The default cost for a 1000 Mbps port is 4, a 100 Mbps port is 19, and for a 10 Mbps port the default cost is 100. priority <value 0-255> – A numeric value between 0 and 255 that is used in determining the root and designated port in an STP port list. The default is 128, with 0 indicating the highest priority. state [enabled/disabled] – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled. 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 0-65535> – A numerical value between 0 and 65535 that is used in determining the root device, root port, and designated port. The device with the

config stp

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

Example Usage:

To set maxage to 18 and hellotime to 4:

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

 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.

enable stp

Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable STP 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:

Status 1: STP enabled:

```
local>show stp
Command: show stp

STP Status                    : Enabled
Max Age                        : 18
Hello Time                     : 4
Forward Delay                  : 15
Priority                      : 32768
Forwarding BPDU                : Enabled
```

```
Designated Root Bridge   : 00-00-00-12-00-00
Root Priority            : 32768
Cost to Root             : 19
Root Port                : 33
Last Topology Change     : 13sec
 Topology Changes Count: 0
```

Status 2: STP Disabled

```
local>show stp
Command: show stp

STP Status         : Disabled
Max Age            : 18
Hello Time         : 4
Forward Delay      : 15
Priority           : 32768
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 beginning port number and the highest port number of the range. The

show stp ports

	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 STP state of port 1-9:

```
local>show stp ports 1-9

Port   Connection       State       Cost      Priority    Status
----   ---------------- ----------- -----     ----------  ---------------
1      Link Down        Enabled     19        128         Forwarding
2      Link Down        Enabled     19        128         Forwarding
3      Link Down        Enabled     19        128         Forwarding
4      Link Down        Enabled     19        128         Forwarding
5      Link Down        Enabled     19        128         Forwarding
6      Link Down        Enabled     19        128         Forwarding
7      Link Down        Enabled     19        128         Forwarding
8      Link Down        Enabled     19        128         Forwarding
9      Link Down        Enabled     19        128         Forwarding
```

10

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
show multicast_fdb	vlan <vlan_name 32> mac_address <macaddr>
config fdb	<sec>

Command	Parameters
aging_time	
show fdb	port <port> vlan <vlan_name 32> mac_address <macaddr> static aging_time
create fdbfilter	<macaddr> [src/dst/either]
delete fdbfilter	<macaddr>
show fdbfilter	{<macaddr>}

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

create fdb

	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.
```

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.

create multicast_fdb	
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

config multicast_fdb	
	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>**
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

config fdb aging_time

	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.

show fdb

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   ALL   BlackHole
 1     default        00-00-00-00-01-02    5    Permanent
 1     default        00-50-BA-6B-2A-29    9    Dynamic
 Total Entries = 3

local>
```

create fdbfilter

Purpose	Used to create a forwarding database table.
Syntax	**create fdbfilter <macaddr> [src/dst/either]**
Description	This command allows MAC addresses to be statically entered into the switch’s MAC Address Filtering Table. These addresses will never age out.
Parameters	<macaddr> – The MAC address that will be added to the forwarding table. src – When *Src* is chosen, packets with the specified MAC address as their source will be dropped. dst – When *Dst* is chosen, packets with the specified MAC address as their destination will be dropped either – When *Either* is chosen, all packets to or from the specific MAC address will be dropped by the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create a forwarding database filter:

```
local>create fdbfilter 01-00-5E-00-00-00 either
Command: create fdbfilter 01-00-5E-00-00-00 either

  Success.

local>
```

delete fdbfilter

Purpose	Used to delete a forwarding database filter.
Syntax	**delete fdbfilter <macaddr>**
Description	This command is used to delete a previously-created forwarding database filter.
Parameters	<macaddr> – The MAC address of the forwarding database filter.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a FDB filter:

```
local>delete fdbfilter 00-00-00-00-01-02
Command: delete fdbfilter 00-00-00-00-01-02

 Success.
```

```
local>
```

show fdbfilter

Purpose	Used to display the current forwarding database filters.
Syntax	**show fdbfilter <macaddr>**
Description	This command will display the current forwarding database filters.
Parameters	<macaddr> – The MAC address of the forwarding table filter.
Restrictions	none.

Example Usage:

To display the switch's fdb filters:

```
local>show fdbfilter
Command: show fdbfilter

 MAC Address Filtering
 MAC Address         Src/Dst
 -------------------------  -----------
 00-00-00-00-01-01    Either

 Total Entries:  1

local>
```

11

BROADCAST STORM CONTROL COMMANDS

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

Command	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.

config 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.

config traffic control

	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

                               Broadcast Multicast  Destination
Group [ports] Threshold Storm      Storm      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

local>
```

12

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_segmentatio n	<portlist> forward_list [null / <portlist>]
show traffic_segmentatio	<portlist>

Command	Parameters
n	
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

config scheduling

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 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

config scheduling

	16 ms to determine the maximum latency. For example, if 3 is specified, the maximum latency allowed will be 3 X 16 = 48 ms. When the specified hardware priority queue has been waiting to transmit packets for this amount of time, the current queue will finish transmitting its current packet, and then allow the hardware priority queue whose max_latency timer has expired to begin transmitting packets.
Parameters	<class_id 0-3> – This specifies which of the four hardware priority queues the config scheduling command will apply to. The four hardware priority queues are identified by number – from 0 to 3 – with the 0 queue being the lowest priority. max_packet <value 0-255> – Specifies the maximum number of packets the above specified hardware priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 255 can be specified. max_latency <value 0-255> – Specifies the maximum amount of time the above specified hardware priority queue will be allowed to transmit packets before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 255 can be specified – with this value multiplied by 16 ms to arrive at the total allowed time for the queue to

config scheduling

	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.

show scheduling

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

config 802.1p user_priority

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-

config 802.1p user_priority

	you want to associate with the <class_id 0-3> (the number of the hardware queue) with. <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**

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_priori y

Purpose	Used to configure the 802.1p default priority settings on the switch. If an untagged

config 802.1p default_priori y

	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>
```

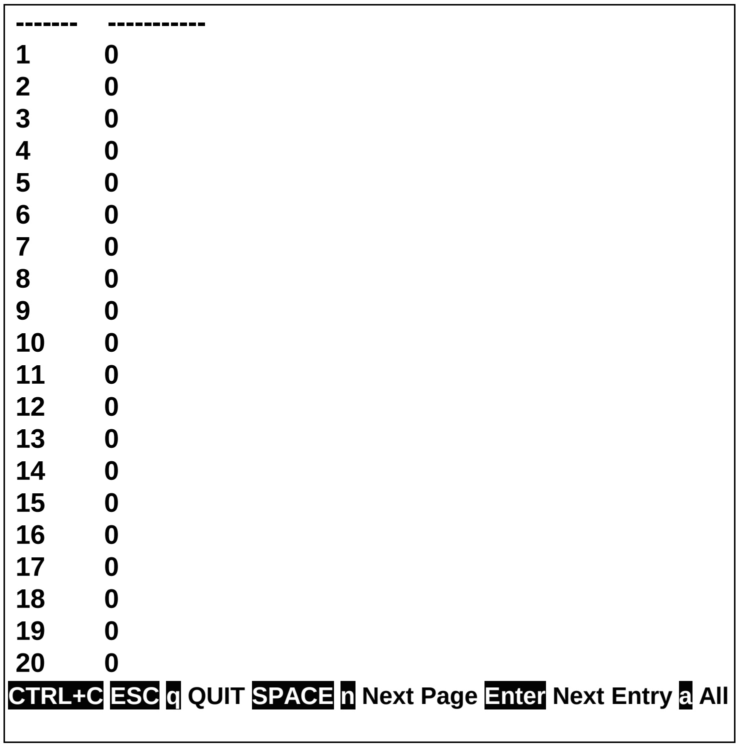
show 802.1p default_priority

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.

config traffic_segmentation	
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.

config bandwidth_control

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

config bandwidth_control

	transmit packets. no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports. <value 1-1000> – Specifies the 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

show 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>
```

13

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 a range of ports to have all of their traffic also sent to a designated port – where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by 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

config mirror port

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

config mirror delete

Purpose	Used to delete a port mirroring configuration/
Syntax	**config mirror <port> delete source <portlist> [rx/tx/both]**
Description	This command is used to delete a previously entered port mirroring configuration.
Parameters	<port> –This specifies the Target port (the port where mirrored packets will be sent).

config mirror delete

	<portlist> – This specifies a range of ports that will be mirrored. That is, a range of ports for which all traffic will be copied and sent to the Target port. 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 delete the mirroring ports:

```
local>config mirror 5 delete source 1-5 both
Command: config mirror 5 delete source 1-5 both
Success.
local>
```

enable mirror

Purpose	Used to enable a previously entered port mirroring configuration.

enable mirror

	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

disable mirror

	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>
```

14

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]**
enable gvrp	
disable gvrp	

Command	Parameters
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

config vlan add

	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.

config vlan delete

	<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]**

config vlan advertisement

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.

config gvrp

Syntax

config gvrp [<portlist>/all] {state [enabled/disabled]/ingress_checking [enabled/disabled] }

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.

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.
```

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

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> – Specifies a range of ports for which the GVRP status is to be displayed. The port list is specified by listing the beginning port number and the highest

show gvrp

	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
```

15

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <value>
delete link_aggregation	group_id <value>
config link_aggregation	group_id <value> 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 <value> algorithm

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 <value>**
Description	This command will create a link aggregation group.
Parameters	<value> – Specifies the group id. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.
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 groı p_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<value> – Specifies the group id. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.
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 <value> {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	<value> – Specifies the group id. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. <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> – Specifies a range of ports that will belong to the link aggregation group. 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

config link_aggregation

	numerical order. state [enabled/disabled] – Allows you to enable or disable the specified link aggregation group.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To define a load-sharing group of ports, group-id 1,master port 17:

```
local>config link_aggregation group_id 1 master_port 17 ports 5-
10
Command: config link_aggregation group_id 1 master_port 17
ports 5-10

 Success.

local>
```

config link_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
Syntax	**config link_aggregation algorithm [mac_source/mac_destination/mac_source_dest/ ip_source/ip_destination/ip_source_dest]**

config link_aggregation algorithm

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 <value>/algorithm}**
Description	This command will display the current link aggregation configuration of the switch.
Parameters	<value> – Specifies the group id. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. algorithm – Allows you to specify the display of link aggregation by the algorithm in use by that group.
Restrictions	none.

Example Usage:

```
local>show link_aggregation
Command: show link_aggregation
```

```
Link Aggregation Algorithm = MAC-source-dest
Group ID      : 1
Master Port    : 17
Member Port   : 5-10,17
Status         : Disabled
Flooding Port  : 5
```

16

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**

config ipif System

	[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>
```

17

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 1-65535> state [enabled/disabled]
config router_ports	<vlan_name 32> [add/delete] <portlist>
enable igmp snooping	forward-mcrouter-only

Command	Parameters
show igmp snooping	**vlan <vlan_name 32>** **group**
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 32>/all] {host_timeout <sec 1-16711450>/router_timeout <sec 1-16711450>/leave_timer <sec 1-16711450>/state [enabled/disabled]}**
Description	This command allows you to configure IGMP snooping on the switch.
Parameters	<vlan_name 32> – The name of the VLAN for which IGMP snooping is to be configured. host_timeout <sec 1-16711450> – Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.

config igmp_snooping

	route_timeout <sec 1-16711450> – 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 1-16711450> – 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 32>/all] {query_interval <sec 1-65535>/max_response_time <sec 1-25>/robustness_variable <value 1-255>/last_member_query_interval <sec 1-65535>/state [enabled/disabled]**
Description	This command configures IGMP snooping querier.
Parameters	<vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured. query_interval <sec 1-65535> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. max_response_time <sec 1-25> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds. robustness_variable <value 1-255> – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the

config igmp_snooping querier

robustness variable is used in calculating the following IGMP message intervals:

- Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).

- Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).

- Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

- By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy.

last_member_query_interval <sec 1-65535> – The maximum amount of time between

config igmp_snooping querier

	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.

config router_ports

Syntax	**config router_ports <vlan_name 32> [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 32> – The name of the VLAN on which the router port resides. <portlist> – Specifies a range of ports which will be configured as router ports. 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 multicast 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 32>}**
Description	This command will display the current IGMP snooping configuration on the switch.
Parameters	<vlan_name 32> – The name of the VLAN for which 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  : Enabled
 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
Total Entries:  1

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 32>}**
Description	This command will display the current IGMP snooping group configuration on the swiTch.
Parameters	<vlan_name 32> – The name of the VLAN for which 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   : 26,7

VLAN Name      : default
Multicast group: 224.0.0.9
MAC address    : 01-00-5E-00-00-09
Reports        : 1
Port Member   : 26,7

VLAN Name      : default
Multicast group: 234.5.6.7
MAC address    : 01-00-5E-05-06-07
Reports        : 1
Port Member    : 26,9

VLAN Name      : default
Multicast group: 236.54.63.75
MAC address    : 01-00-5E-36-3F-4B
Reports        : 1
Port Member    : 26,7

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

VLAN Name      : default
Multicast group: 239.255.255.254
MAC address    : 01-00-5E-7F-FF-FE
Reports        : 1
Port Member    : 26,7

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 32>} {static/dynamic}**

Description — This command will display the router ports currently configured on the switch.

Parameters — <vlan_name 32> – The name of the VLAN on which the router port resides.

static – Displays router ports that have been statically configured.

dynamic – Displays router ports that have been dynamically configured.

Restrictions — none.

Example Usage:

To display the router ports.

```
local>show router_ports
Command: show router_ports

 VLAN Name            : default
 Static router port   :
 Dynamic router port:

 Total Entries: 1
```

```
local>
```

18

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.

create iproute

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
```

19

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.

Usage Example

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 account
config bandwidth_control
config command_history
config command_prompt
config fdb aging_time
config gvrp
config igmp_snooping
config igmp_snooping querier
config ipif System
config link_aggregation algorithm
config link_aggregation group_id
config mirror port
config multicast_fdb
config ports
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.

Usage Example:

To display the command history:

```
local>show command_history
Command: show command_history
show
?
config command_history
config
?
dir
show command_history
show command_history
```

```
show

config router_ports vlan2 add 1-10
config router_ports vlan2 add
config router_ports vlan2
config router_ports
show vlan
create vlan vlan2 tag 3
create vlan vlan2 tag 2
show router_ports
show router ports
login
local>
```

dir

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

Usage Example

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 account
config bandwidth _control
config command history
config command_prompt
config fdb aging_time
config gvrp
config igmp_snooping
config igmp_snooping querier
config ipif System
config link_aggregation algorithm
config link_aggregation group_id
config mirror port
config multicast_fdb
config ports
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.

Usage Example

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 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 Nway auto-negotiation	
Protocols:	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	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 Enviroı mental
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
Dimensions:	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width

	Physical and Environmental
	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 overlaped!”	
74	"Default VLAN can't be deleted.”	
75	"VLAN name overlaped!”	
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): 1800-177100
TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au
E-MAIL: support@dlink.com.au & info@dlink.com.au

Level 1, 434 St. Kilda Road, Melbourne,
Victoria 3004 Australia
TEL: 61-3-9281-3232 FAX: 61-3-9281-3229
MOBILE: 0412-660-064

Canada

D-Link Canada
2180 Winston Park Drive, Oakville,
Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5095
BBS: 1-965-279-8732
TOLL FREE: 1-800-354-6522 URL: www.dlink.ca
FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca

Chile

D-Link South America
Isidora Goyenechea 2934 Of. 702, Las Condes Fono,
2323185, Santiago, Chile, S. A.
TEL: 56-2-232-3185 FAX: 56-2-232-0923
URL: www.dlink.cl
E-MAIL: ccasassu@dlink.cl & tsilva@dlink.cl

China

D-Link China
15th Floor, Science & Technology Tower, No.11,
Baishiqiao Road, Haidan District, 100081 Beijing, China
TEL: 86-10-68467106 FAX: 86-10-68467110
URL: www.dlink.com.cn
E-MAIL: liweii@digitalchina.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: 20-2-635-6176 FAX: 20-2-635-6192
URL: www.dlink-me.com
E-MAIL: support@dlink-me.com & fateen@dlink-me.com

Finland **D-Link Finland**
Pakkalankuja 7A, FIN– 0150 VANTAA, Finland
TEL: 358-9-2707-5080 FAX: 358-9-2702-5081
URL: www.dlink-fi.com

France **D-Link France**
Le Florilege, No. 2, Allea 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
URL: www.dlink.de
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 E-MAIL: info@dlink.de

India **D-Link India**
Plot No.5, Bandra-Kurla Complex Rd., Off Cst Rd.,
Santacruz (East), Mumbai, 400 098 India
TEL: 91-022-652-6696/6578/6623
FAX: 91-022-652-8914/8476
URL: www.dlink-india.com, www.dlink.co.in &
tushars@dlink-india.com E-MAIL: service@dlink.india.com

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 Nishigotahda, Shinagawa, 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**
Fellenoord 1305611 ZB, Eindhoven, the Netherlands
TEL: 31-40-2668713 FAX: 31-40-2668666
URL: www.d-link-benelux.nl

Norway **D-Link Norway**
Waldemar Thranesgate 77, 0175 Oslo, Norway
TEL: 47-22-991890 FAX: 47-22-207039
URL: www.dlink.no

Russia **D-Link Russia**
Michurinski Prospekt 49, 117607 Moscow, Russia
TEL: 7-095-737-3389 & 7-095-737-3492
FAX: 7-095-737-3390 URL: www.dlink.ru
E-MAIL: vl@dlink.ru

Singapore **D-Link International**
International Business Park, #03-12 The Synergy,
Singapore 609917
TEL: 65-774-6233 FAX: 65-774-6322
E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com

South Africa **D-Link South Africa**
Unit 2, Parkside, 86 Oak Avenue, Highveld Technopark,
Centurion, Gauteng, South Africa
TEL: 27 (0) 12-665-2165 FAX: 27 (0) 12-665-2186
URL: www.d-link.co.za E-MAIL: attie@d-link.co.za

Spain **D-Link Iberia**
C/Sabino De Arana, 56 Bajos, 08028 Barcelona, Spain
TEL: 34 93 4090770 FAX: 34 93 4910795
URL: www.dlinkiberia.es E-MAIL: info@dlinkiberia.es

Sweden **D-Link Sweden**
P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-(0) 8-564-61900 FAX: 46-(0) 8-564-61901
E-MAIL: info@dlink.se URL: www.dlink.se

Taiwan **D-Link Taiwan**
2F, No. 233-2 Pao-chiao Rd, Hsin-tien, Taipei, Taiwan
TEL: 886-2-2916-1600 FAX: 886-2-2914-6299
URL: www.dlink.com.tw E-MAIL: dssqa@tsc.dlinktw.com.tw

Turkey **D-Link Middle East**
Deniz Bilgisayar, Buyukdere Cad. Naci Kasim Sk., No. 5
Mecidiyekoy, Istanbul, Turkey
TEL: 90-212-213-3400 FAX: 90-212-213-3420
E-MAIL: smorovati@dlink-me.com

U.A.E. **D-Link Middle East**
CHS Aptec (Dubai), P.O. Box 33550 Dubai U.A.E.
TEL: 971-4-366-885 FAX: 971-4-355-941
E-MAIL: Wxavier@dlink-me.com

U.K. **D-Link Europe**
4th Floor, Merit House, Edgware Road, Colindale, London
NW9 5AB United Kingdom
TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511
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
BBS: 1-949-455-1779 & 1-949-455-9616
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®